NK 10/019893

Copy for the Elected Office (EO/US)

PCT/FI00/00513

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

JOHANSSON, Folke
Nokia Corporation
P.O. Box 226
FIN-00045 Nokia Group
FINLANDE

RECEIVED
MAY 1 0 2002
Technology Center 2600

Date of mailing (day/month/year)	IMPORTANT NOTIFICATION
22 janvier 2002 (22.01.02)	
Applicant's or agent's file reference 27008 WO	
International application No. PCT/FI00/00513	**International filing date** (day/month/year) 07 juin 2000 (07.06.00)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address	State of Nationality	State of Residence
JOHANSSON, Folke Nokia Corporation P.O. Box 206 FIN-00045 Nokia Group Finland		
	Telephone No. +358 7180-08000	
	Facsimile No. +358 7180-62919	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address	State of Nationality	State of Residence
JOHANSSON, Folke Nokia Corporation P.O. Box 226 FIN-00045 Nokia Group Finland		
	Telephone No. +358 7180-08000	
	Facsimile No. +358 7180-62919	
	Teleprinter No.	

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Beate GIFFO-SCHMITT
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

Form PCT/IB/308 (March 1994)

004608043

Best Available Copy

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

JOHANSSON, Folke
Nokia Corporation
P.O. Box 206
FIN-00045 Nokia Group
FINLANDE

Date of mailing (day/month/year)
17 April 2001 (17.04.01)

Applicant's or agent's file reference
27008 WO

IMPORTANT NOTIFICATION

International application No.
PCT/FI00/00513

International filing date (day/month/year)
07 June 2000 (07.06.00)

1. The following indications appeared on record concerning:

☐ the applicant ☐ the inventor ☒ the agent ☐ the common representative

Name and Address

JOHANSSON, Folke
Nokia Corporation
P.O. Box 319
FIN-00045 Nokia Group
Finland

State of Nationality

State of Residence

Telephone No.
+358 9 51121

Facsimile No.
+358 9 511 64604

Teleprinter No.

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

☐ the person ☐ the name ☒ the address ☐ the nationality ☐ the residence

Name and Address

JOHANSSON, Folke
Nokia Corporation
P.O. Box 206
FIN-00045 Nokia Group
Finland

State of Nationality

State of Residence

Telephone No.
+358 7180-08000

Facsimile No.
+358 7180-62919

Teleprinter No.

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

☒ the receiving Office
☐ the International Searching Authority
☒ the International Preliminary Examining Authority
☐ the designated Offices concerned
☒ the elected Offices concerned
☐ other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

F. Baechler

Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 07 March 2001 (07.03.01)	
International application No. PCT/FI00/00513	**Applicant's or agent's file reference** 27008 WO
International filing date (day/month/year) 07 June 2000 (07.06.00)	**Priority date** (day/month/year) 30 June 1999 (30.06.99)
Applicant SOLALA, Erkki	

1. The designated Office is hereby notified of its election made:

   [X] in the demand filed with the International Preliminary Examining Authority on:

   18 January 2001 (18.01.01)

   [ ] in a notice effecting later election filed with the International Bureau on:

   _____

2. The election [X] was

   [ ] was not

   made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer R. E. Stoffel Telephone No.: (41-22) 338.83.38

Form PCT/IB/331 (July 1992)

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
NOKIA CORPORATION
Attn. JOHANSSON, Folke
P.O. Box 319
00045 Nokia Group
FINLAND

01. 12. 01

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION

(PCT Rule 44.1)

Applicant's or agent's file reference 27008 WO	Date of mailing *(day/month/year)* 29/11/2000
International application No. PCT/FI 00/00513	**FOR FURTHER ACTION** See paragraphs 1 and 4 below
Applicant NOKIA CORPORATION et al.	International filing date *(day/month/year)* 07/06/2000

1. [X] The applicant is hereby notified that the International Search Report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the International Search Report; however, for more details, see the notes on the accompanying sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Fascimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no International Search Report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. [ ] **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

[ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

[ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

Within **19 months** from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within **20 months** from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Theresia Van Deursen

Form PCT/ISA/220 (July 1998)

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the PCT Applicant's Guide, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped),whether

(i) the claim is unchanged;

(ii) the claim is cancelled;

(iii) the claim is new;

(iv) the claim replaces one or more claims as filed;

(v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."

2. [Where originally there were 15 claims and after amendment of all claims there are 11]:
"Claims 1 to 15 replaced by amended claims 1 to 11."

3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."

4. [Where various kinds of amendments are made]:
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

"Statement under article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments and any accompanying statement, under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the time of filing the amendments (and any statement) with the International Bureau, also file with the International Preliminary Examining Authority a copy of such amendments (and of any statement) and, where required, a translation of such amendments for the procedure before that Authority (see Rules 55.3(a) and 62.2, first sentence). For further information, see the Notes to the demand form (PCT/IPEA/401).

Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see Volume II of the PCT Applicant's Guide.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
27008 WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/FI 00/00513	07/06/2000	30/06/1999
Applicant		
NOKIA CORPORATION et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

[ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

[ ] contained in the international application in written form.

[ ] filed together with the international application in computer readable form.

[ ] furnished subsequently to this Authority in written form.

[ ] furnished subsequently to this Authority in computer readble form.

[ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

[ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

[X] the text is approved as submitted by the applicant.

[ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

[X] the text is approved as submitted by the applicant.

[ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 4

[X] as suggested by the applicant.

[ ] None of the figures.

[ ] because the applicant failed to suggest a figure.

[ ] because this figure better characterizes the invention.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
27008 WO		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/FI 00/00513	07/06/2000	30/06/1999
Applicant		
NOKIA CORPORATION et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

   a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

   [ ] contained in the international application in written form.

   [ ] filed together with the international application in computer readable form.

   [ ] furnished subsequently to this Authority in written form.

   [ ] furnished subsequently to this Authority in computer readble form.

   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. [ ] **Certain claims were found unsearchable** (See Box I).

3. [ ] **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

   [X] the text is approved as submitted by the applicant.

   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 4

   [X] as suggested by the applicant.

   [ ] because the applicant failed to suggest a figure.

   [ ] because this figure better characterizes the invention.

   [ ] None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FI 00/00513

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	WO 99 56431 A (NOKIA MOBILE PHONES LTD (F) 4 November 1999 (1999-11-04) page 5, line 13 -page 9, line 7; figure 3 abstract; claims 1-4	1-4, 6-14, 16-20
Y	---	5,15
Y	PATENT ABSTRACTS OF JAPAN vol. 1998, no. 10, 31 August 1998 (1998-08-31) & JP 10 136336 A (CANON INC), 22 May 1998 (1998-05-22) abstract	5,15

A	EP 0 642 283 A (NOKIA MOBILE PHONES LTD) 8 March 1995 (1995-03-08) page 1, line 1 -page 2, line 24 abstract	1-20

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 October 2000	29. 11. 2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Thomas Tholin

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FI 00/00513

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9956431 A	04-11-1999	AU 4360999 A	16-11-1999
JP 10136336 A	22-05-1998	US 6088737 A	11-07-2000
EP 0642283 A	08-03-1995	FI 933894 A	07-03-1995
		JP 7170579 A	04-07-1995
		US 5802465 A	01-09-1998

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

(PCT Rule 47.1(c), first sentence)

To:
JOHANSSON, Folke
Nokia Corporation
P.O. Box 319
FIN-00045 Nokia Group
FINLANDE

19. 01. 2001

Date of mailing (day/month/year)	
11 January 2001 (11.01.01)	
Applicant's or agent's file reference	**IMPORTANT NOTICE**
27008 WO	

International application No.	International filing date (day/month/year)	Priority date (day/month/year)
PCT/FI00/00513	07 June 2000 (07.06.00)	30 June 1999 (30.06.99)

Applicant
NOKIA CORPORATION et al

1. Notice is hereby given that the International Bureau has communicated, as provided in Article 20, the international application to the following designated Offices on the date indicated above as the date of mailing of this Notice:
   AG,AU,DZ,KP,KR,MZ,US

   In accordance with Rule 47.1(c), third sentence, those Offices will accept the present Notice as conclusive evidence that the communication of the international application has duly taken place on the date of mailing indicated above and no copy of the international application is required to be furnished by the applicant to the designated Office(s).

2. The following designated Offices have waived the requirement for such a communication at this time:
   AE,AL,AM,AP,AT,AZ,BA,BB,BG,BR,BY,CA,CH,CN,CR,CU,CZ,DE,DK,DM,EA,EE,EP,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,NO,NZ,OA,PL,PT,RO,RU,SD,SE,SG,SI,SK,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW
   The communication will be made to those Offices only upon their request. Furthermore, those Offices do not require the applicant to furnish a copy of the international application (Rule 49.1(a-bis)).

3. Enclosed with this Notice is a copy of the international application as published by the International Bureau on
   11 January 2001 (11.01.01) under No. WO 01/03368

REMINDER REGARDING CHAPTER II (Article 31(2)(a) and Rule 54.2)

If the applicant wishes to postpone entry into the national phase until 30 months (or later in some Offices) from the priority date, **a demand for international preliminary examination** must be filed with the competent International Preliminary Examining Authority before the expiration of 19 months from the priority date.

It is the applicant's sole responsibility to monitor the 19-month time limit.

Note that only an applicant who is a national or resident of a PCT Contracting State which is bound by Chapter II has the right to file a demand for international preliminary examination.

REMINDER REGARDING ENTRY INTO THE NATIONAL PHASE (Article 22 or 39(1))

If the applicant wishes to proceed with the international application in the **national phase**, he must, within 20 months or 30 months, or later in some Offices, perform the acts referred to therein before each designated or elected Office.

For further important information on the time limits and acts to be performed for entering the national phase, see the Annex to Form PCT/IB/301 (Notification of Receipt of Record Copy) and Volume II of the PCT Applicant's Guide.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer
J. Zahra

Telephone No. (41-22) 338.83.38

Continuation of Form PCT/IB/308

NOTICE INFORMING THE APPLICANT OF THE COMMUNICATION OF THE INTERNATIONAL APPLICATION TO THE DESIGNATED OFFICES

Date of mailing (day/month/year)	IMPORTANT NOTICE
11 January 2001 (11.01.01)	
Applicant's or agent's file reference	**International application No.**
27008 WO	PCT/FI00/00513

The applicant is hereby notified that, at the time of establishment of this Notice, the time limit under Rule 46.1 for making amendments under Article 19 has not yet expired and the International Bureau had received neither such amendments nor a declaration that the applicant does not wish to make amendments.

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

JOHANSSON, Folke
Nokia Corporation
P.O. Box 206
FIN-00045 Nokia Group
FINLANDE

03 04. 2001

Date of mailing (day/month/year) 17 April 2001 (17.04.01)	
Applicant's or agent's file reference 27008 WO	**IMPORTANT NOTIFICATION**
International application No. PCT/FI00/00513	**International filing date** (day/month/year) 07 June 2000 (07.06.00)

1. The following indications appeared on record concerning:

[ ] the applicant [ ] the inventor [X] the agent [ ] the common representative

Name and Address	State of Nationality	State of Residence
JOHANSSON, Folke Nokia Corporation P.O. Box 319 FIN-00045 Nokia Group Finland		
	Telephone No. +358 9 51121	
	Facsimile No. +358 9 511 64604	
	Teleprinter No.	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address	State of Nationality	State of Residence
JOHANSSON, Folke Nokia Corporation P.O. Box 206 FIN-00045 Nokia Group Finland		
	Telephone No. +358 7180-08000	
	Facsimile No. +358 7180-62919	
	Teleprinter No.	

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[X] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland** Facsimile No.: (41-22) 740.14.35	Authorized officer F. Baechler Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994)

003967566

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

INFORMATION CONCERNING ELECTED OFFICES NOTIFIED OF THEIR ELECTION

(PCT Rule 61.3)

To:

JOHANSSON, Folke
Nokia Corporation
P.O. Box 319
FIN-00045 Nokia Group
FINLANDE

15. 03. 2001

Date of mailing (day/month/year) 07 March 2001 (07.03.01)	
Applicant's or agent's file reference 27008 WO	**IMPORTANT INFORMATION**

International application No.	**International filing date** (day/month/year)	**Priority date** (day/month/year)
PCT/FI00/00513	07 June 2000 (07.06.00)	30 June 1999 (30.06.99)

Applicant
NOKIA CORPORATION et al

1. The applicant is hereby informed that the International Bureau has, according to Article 31(7), notified each of the following Offices of its election:

   AP :GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZW
   EP :AT,BE,CH,CY,DE,DK,ES,FI,FR,GB,GR,IE,IT,LU,MC,NL,PT,SE
   National :AU,BG,CA,CN,CZ,DE,IL,JP,KP,KR,MN,NO,NZ,PL,RO,RU,SE,SK,US

2. The following Offices have waived the requirement for the notification of their election; the notification will be sent to them by the International Bureau only upon their request:

   EA :AM,AZ,BY,KG,KZ,MD,RU,TJ,TM
   OA :BF,BJ,CF,CG,CI,CM,GA,GN,GW,ML,MR,NE,SN,TD,TG
   National :AE,AG,AL,AM,AT,AZ,BA,BB,BR,BY,CH,CR,CU,DK,DM,DZ,EE,ES,FI,GB,GD,
   GE,GH,GM,HR,HU,ID,IN,IS,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MW,MX,
   MZ,PT,SD,SG,SI,SL,TJ,TM,TR,TT,TZ,UA,UG,UZ,VN,YU,ZA,ZW

3. The applicant is reminded that he must enter the "national phase" **before the expiration of 30 months from the priority date** before each of the Offices listed above. This must be done by paying the national fee(s) and furnishing , if prescribed, a translation of the international application (Article 39(1)(a)), as well as, where applicable, by furnishing a translation of any annexes of the international preliminary examination report (Article 36(3)(b) and Rule 74.1).

   Some offices have fixed time limits expiring later than the above-mentioned time limit. For detailed information about the applicable time limits and the acts to be performed upon entry into the national phase before a particular Office, see Volume II of the PCT Applicant's Guide.

   The entry into the European regional phase is postponed **until 31 months from the priority date** for all States designated for the purposes of obtaining a European patent.

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. (41-22) 740.14.35

Authorized officer:
R. E. Stoffel

Telephone No. (41-22) 338.83.38

PATENTTI- REKISTERIHALLITUS

VÄLIPÄÄTÖS

10/019893

531 Rec'd PCT/F 28 DEC 2001

30.08.2000

01.09.2000

Nokia IPR-osasto

PL 319

00045 Nokia Group

Patenttihakemus nro:	991493
Luokka:	H04L / OPS
Hakija:	Nokia Corporation
Asiamies:	
Asiamiehen viite:	27006 FI
Määräpäivä:	28.02.2001

Patenttihakemuksen numero ja luokka on mainittava kirjelmässänne PRH:lle

Hakemuksen kohteena oleva keksintö on suoritetun tutkimuksen perusteella patentoitavissa (patenttilaki 1 ja 2 §).

Tekniikan tasona viitataan seuraaviin julkaisuihin: US-A-5485460 (G06F 13/00, Microsoft Corp.), jossa on kuvattu laite ja menetelmä jossa käytetään kahta protokollapinoa. Tuleva paketti tarkastetaan etukäteen ja ohjataan oikeaan pinoon. Julkaisussa ei kuitenkaan ole mainintaa käyttöoikeuksien tarkistamisesta tässä yhteydessä; US-A-5915087 (G06F 11/00, Secure Computing Corp.), jossa on kuvattu menetelmä palvelimen käyttöoikeuksien tarkistamiseksi erillisen välityspalvelin avulla.

Hakemusta tulisi täydentää suomenkielisillä selityksellä, vaatimuksilla ja tiivistelmällä, sekä ruotsinkielisillä vaatimuksilla ja tiivistelmällä. Käännösten mukana tulee olla hakijan tai asiamiehen vakuutus, että käännökset vastaavat alkuperäisiä asiakirjoja. (Patenttimääräys 38a § 3 mom.)

Olli Sievänen

Tutkijainsinööri Olli-Pekka Sievänen
Puhelin: (09) 6939 5438

Liite: kopiot viitejulkaisuista ja tutkimusraportista

Lausumanne huomautusten johdosta on annettava viimeistään yllämainittuna määräpäivänä. Jollette ole antanut lausumaanne virastoon viimeistään mainittuna määräpäivänä tai ryhtynyt toimenpiteisiin tässä välipäätöksessä esitettyjen puutteellisuuksien korjaamiseksi, jätetään hakemus sillensä (patenttilain 15 §). Sillensä jätetty hakemus otetaan uudelleen käsiteltäväksi, jos Te neljän kuukauden kuluessa määräpäivästä annatte lausumanne tai ryhdytte toimenpiteisiin esitettyjen puutteellisuuksien korjaamiseksi ja samassa ajassa suoritatte vahvistetun maksun, 320 mk hakemuksen ottamisesta uudelleen käsiteltäväksi. Jos lausumanne on annettu virastoon oikeassa ajassa, mutta esitettyjä puutteellisuuksia ei ole siten korjattu, että hakemus voitaisiin hyväksyä, se hylätään, mikäli virastolla ei ole aihetta antaa Teille uutta välipäätöstä (patenttilain 16 §). Uusi keksinnön selitys, siihen tehdyt lisäykset ja uudet patenttivaatimukset on aina jätettävä kahtena kappaleena ja tällöin on otettava huomioon patenttiasetuksen 19 §.

Postiosoite: Pl 1160, 00101 Helsinki
Katuosoite: Arkadiankatu 6 A, 00100 Helsinki
Puhelin: (09) 6939500
Telefax: (09) 69395328
Pankki: Leonia 800015-47908

10/019893

PATENTTI- JA REKISTERIHALLITUS
Patentti- ja innovaatiolinja

TUTKIMUSRAPORTTI

531 Rec'd PCT/ 28 DEC 2001

PATENTTIHAKEMUS NRO	LUOKITUS
991493	H04L 9/32, H04L 29/06

TUTKITTU AINEISTO

Patenttijulkaisukokoelma (FI, SE, NO, DK, DE, CH, EP, WO, GB, US), tutkitut luokat

H04L 9/32, H04L 29/06

Tiedonhaut ja muu aineisto

EPODOC, WPI

VIITEJULKAISUT

Kategoria*)	Julkaisun tunnistetiedot	Koskee vaatimuksia
A	US-A-5485460, G06F 13/00, Microsoft Corp.	1,11,20
A	US-A-5915087, G06F 11/00, Secure Computing Corp.	1,11,20

*) X Patentoitavuuden kannalta merkittävä julkaisu yksinään tarkasteltuna
Y Patentoitavuuden kannalta merkittävä julkaisu, kun otetaan huomioon tämä ja yksi tai useampi samaan kategoriaan kuuluva julkaisu
A Yleistä tekniikan tasoa edustava julkaisu, ei kuitenkaan patentoitavuuden este

Päiväys	Tutkija
30.8.00	Olli-Pekka Sievänen

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:

JOHANSSON, Folke
NOKIA CORPORATION
P.O. Box 319
00045 Nokia Group
FINLANDE

05. 11. 2001
Comp. record
Prior Art/2111
Prior Art/103
Attorney
CC:

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT
(PCT Rule 71.1)

Date of mailing *(day/month/year)*	30.10.2001
Applicant's or agent's file reference 27008 WO	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/FI00/00513	07/06/2000	30/06/1999

Applicant
NOKIA CORPORATION et al.

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/	Authorized officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Barrio Baranano, A Tel.+49 89 2399-8621

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
27008 WO		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/FI00/00513	07/06/2000	30/06/1999
International Patent Classification (IPC) or national classification and IPC H04L12/00		
Applicant NOKIA CORPORATION et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 22 sheets. + 1 Document (2 pages) cited in Report

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   - VI ☒ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
18/01/2001	30.10.2001
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Lebas, Y Telephone No. +49 89 2399 8980

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/FI00/00513

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:
Description, pages:

1-17	as received on	21/08/2001	with letter of	20/08/2001

Claims, No.:

1-20	as received on	21/08/2001	with letter of	20/08/2001

Drawings, sheets:

1/4-4/4	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

   ☐ the language of publication of the international application (under Rule 48.3(b)).

   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority in written form.

   ☐ furnished subsequently to this Authority in computer readable form.

   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:

   ☐ the claims, Nos.:

☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

(Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-20
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1-20
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations
see separate sheet

VI. Certain documents cited

1. Certain published documents (Rule 70.10)

and / or

2. Non-written disclosures (Rule 70.9)

see separate sheet

Cited Document:

D1: "Sicherheitskonzepte für das Internet" from Martin Raepple, ISBN 3-932588-14-2, published in 1998 by Dpunkt-Verlag, pages 167-170.

Document D1 was not cited in the international search report. A copy of this document is appended hereto (with a copy that shows the actual publication date of D1).

Re Item V

Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. The present application relates to a method of controlling, at a server, access right of a message (data packet) received from a terminal at the server.

   In this method, a session is established between the server and the terminal for receiving the data packets. The checking of the access right is done, before the packet is allowed to pass the protocol stack of the server, by:

   storing a number (Y) of access right licenses purchased by a licensee;
   reserving a license (C) of the licensee if the data packet arrived in a new concurrent session relating to the licensee; and
   controlling that the number of reserved licenses (C) does not exceed the number of purchased access right licenses (Y).

   D1, which is considered as the closest prior art, discloses a method for checking at a screening router which packets are allowed to pass on to the protocol stack. The method of the application differs from the disclosure of D1 in that it furthermore checks the access right of a data packet by controlling the number of licenses purchased by a licensee involved in the session between server and terminal.

   This method allows a more thorough controlling of data packet access right received from a terminal at a server.

   As there is no indication in D1 or in any of the prior art documents to improve the

method of D1 to arrive at the method of the Application, this method can be regarded as inventive.

D2 discloses a camera server that controls access to video data by comparing the number of connected clients to a permissible number.

Independent claim 1 relates to the method.
Independent claim 11 is a claim for a server adapted to perform all the steps of the method of claim 1.
Independent claim 20 is a claim for a computer program product at a server, comprising computer readable program means for causing the server to perform all the steps of the method of claim 1.

As for claim 1, claims 11 and 20 meet the PCT requirements for novelty and inventive step (Articles 33(1)-(3) PCT).

2. Claims 2-10 and 12-19, depending respectively on independent claims 1 and 11, also meet the requirements for novelty and inventive step (Articles 33(1)-(3) PCT).

Re Item VI
Certain document cited

Certain published document (Rule 70.10)

Application No Patent No	Publication date *(day/month/year)*	Filing date *(day/month/year)*	Priority date *(valid claim)* *(day/month/year)*
WO 99/56431A	04/11/99	27/04/99	28/04/98

Document WO 99/56431A is not comprised within the state of the art relevant to the application.
However, if the Applicant decided to apply for a European Patent, this document would become relevant in the European phase for the evaluation of the novelty of the Application.

10/019893
1 531 Rec'd PCT/PT 28 DEC 2001

License control at a gateway server

The present invention relates to license control at a gateway server for controlling the right for a message to enter the server. It is particularly suitable for a mobile protocol such as WAP (Wireless Application Protocol) for enabling a mobile terminal to access the Internet via the gateway server.

The term "Internet" is commonly used to describe information, content, which can be accessed using a terminal, typically a PC, connected via a modem to a telecommunications network. The content can be stored at many different sites remote from the accessing computer, although each of the remote sites is also linked to the telecommunications network. The content can be structured using HyperText Mark-up Language (HTML). The Internet is made workable by the specification of a standard communications system which makes use of a number of protocols, such as the Transfer Control Protocol (TCP), the User Datagram Protocol (UDP), and the Internet Protocol (IP), to control the flow of data around the numerous different components of the Internet. TCP and UDP are concerned with the prevention and correction of errors in transmitted Internet data. IP is concerned with the structuring and routing of data. On top of that, other application specific protocols may be provided to manage and manipulate the various kinds of information available via the Internet, for example HTTP to access HTML content, FTP to access files or SMTP to access e-mail.

The Internet is physically constructed from a hierarchy of telecommunication and data communication networks, for example local area networks (LANs), regional telephone networks, and international telephone networks. These networks are connected internally and externally by so-called "routers" which receive data from a source host, or a previous router in a transmission chain, and route it to the destination host or the next router in the transmission chain.

With increased use of mobile cellular telephones, there is a growing demand for so-called mobile Internet access, in which access is made from a portable

computer connected to a cellular telephone or from an integrated computer/cellular phone device. Typically, the purpose of such access is to obtain content from the Internet. It has also been proposed to provide Internet access to advanced mobile terminals, so-called communicators and smart phones, by means of the Wireless Application Protocol (WAP), for example. WAP has an architecture in which there is a protocol stack having an application layer (called the Wireless Application Environment or WAE), a session layer (called the Wireless Session Protocol or WSP), a transaction layer (called the Wireless Transaction Protocol or WTP), a security layer (called Wireless Transport Layer Security or WTLS) and a transport layer (called the Wireless Datagram Protocol or WDP) as shown in Figure 1. Each of the layers of the architecture is accessible by the layers above as well as by other services and applications. These protocols are designed to operate over a variety of different bearer services such as SMS (Short Message Service), CSD (Circuit Switched Data), GPRS (General Packet Radio Service) etc. A specification describing the WAP architecture and the protocol layers is available from http//www.wapforum.org/.

Obtaining access to the Internet generally involves having sessions between a terminal, such as a mobile terminal, and a server. A session is a series of interactions between a terminal and a server having a well-defined beginning and end and involving agreed-upon characteristics. Typically, a session involves a peer announcing to another peer a desire to establish a session, both peers negotiating the characteristics of the session, the peers engaging in a variety of transactions and one of the peers ending the session. The characteristics which are negotiated are typically the length of packets to be exchanged, the character sets which can be understood and manipulated and the versions of protocols which are to be used. A transaction is a basic unit of interaction and may include requesting and receiving information, aborting an ongoing session and informing a peer of a situation in an on-going session. All session operations to establish and terminate a session as well as all transactions result in events being generated and received by the peer. There are many event sources (sessions and transactions).

The operations which an application can invoke to generate events are called service primitives. Service primitives represent the logical exchange of information and control between the session layer and other layers. They consist of commands and their respective responses associated with the particular service provided. Invoking a service primitive in a peer on one side of a communication link results in an event being generated in a peer in the other side of the link. Service primitives are present in all communication protocols.

An active session can involve multiple transactions and so can generate multiple events. Depending on the speed at which an application can process events coming from its peer, it can happen that there are more transactions than it can process and so it receives more events than it can process. In this case, the events are queued up and wait to be processed within the context of that session. Events connected or related to the same session generally need to be processed in a specific order. In some protocols, a session can be suspended, in which state no transactions are allowed except a request to resume or to terminate.

In WAP, communication between layers and between entities within the session layer are also accomplished by means of service primitives.

Most transactions are either of the push type or of the pull (request-reply) type. In push type transactions a peer sends information which has not been specifically requested and in pull type transactions, a peer specifically requests to receive information from another peer.

Terminals, such as personal computers, obtain information from the Internet through a server, such as a gateway server. The Internet uses HTTP which is a simple request-reply protocol. Almost the only event is an HTTP request. The operating system of the server runs a number of applications and so creates a number of threads to deal with them, for example proxies and mail servers. The applications use the available threads as they are required. In the case of Internet

access by a PC, it is convenient to create a thread in the server dynamically to deal with each request because the requests are independent from each other. Once the request has been processed, the thread has finished its activity and is terminated.

In a communication system comprising a gateway server and a plurality of mobile terminals, establishing a session requires a relatively large amount of bandwidth because a terminal and a server must negotiate many characteristics relevant to the session. Furthermore, information which is unique to a particular opened session may be lost if the session is terminated. This unique information could have been negotiated as a result of transactions. For example, it may be the status of a game. In order to avoid opening and closing sessions on demand and establishing new sessions whenever they are needed, the sessions may be kept open for a long time, even in an inactive state, so that they can be resumed when needed. A session can remain open for days or even weeks until it is closed or until the terminal no longer receives power, for example from a battery. An application in the server will use the operating system thread management service and create a number of threads to manage these sessions.

In WAP typically a gateway server will be the port for allowing a terminal to access the Internet. The gateway server will be provided by e.g. a service provider, and users may access the gateway server by purchasing a license or number of licenses from the service provider. Accordingly, there is a need to implement a solution at the gateway server for controlling access to the gateway server. Equally the gateway server is usually implemented as a computer program which when loaded into a computer works as a gateway server. Thereby the manufacturer of the gateway server, i.e. the maker of the computer program, may sell licenses to the service provider, which limits the number of users that the service provider is able to serve without purchasing additional licenses from the manufacturer. Thus there is a need to implement a solution at the gateway server for controlling number of total licenses in use at the server.

In "Sicherheitskonzepte für das Internet" from Martin Raepple, ISBN 3-932588-14-2, edited in 1998 by Dpunkt-Verlag on pages 167-170 discusses a screening router in which there is a check to see which packets are allowed to pass the router (and which not) and in which direction. The sreening router makes a variant of a firewall and the check is performed because of security reasons and at a network layer.

Now a gateway server has been invented where license control is performed on a message entering the gateway server before it is allowed to pass on to the protocol stack, i.e. license control is performed below the protocol stack in the gateway server hierarchy. Identification of the sender of the message is checked to determine access rights. In a WAP gateway or proxy server there is more specifically provided below the WAP stack and above the bearers a bearer gate which performs the license control, and through which all data traffic coming from the bearers passes before going to the protocol stack.

The present invention can be used for controlling access right of a message in both of the above mentioned situations, namely for controlling that the service provider does not exceed the number of licenses it has purchased from the manufacturer of the gateway server and for controlling that a user entity having purchased a number of licenses from the service provider does not exceed that number of licenses.

In a preferred embodiment of the invention datagrams or data packets are received via a particular bearer. This data packet has an address of the sender, also called source address, remote address or client address. Moreover, each data packet has a port number of the sender, also called source port, remote port or client port information. In an embodiment of the present invention both the address and port number of the sender are checked for identifying the sender for license control purposes.

Licenses are calculated on a session basis, i.e. controlling concurrent sessions from the same license holder. There is no limit for number of transactions that are allowed during a session per license, but the license control is about how many sessions are allowed to execute transactions concurrently. In a particular embodiment the sessions will be given a time window during which the license is reserved, and unless there is data traffic within that session within the time window, the license for that session will be released. Next time there is a need for executing transactions within that session, a new license needs to be taken into use.

According to a first aspect of the invention there is provided a server for receiving a message from a terminal and comprising a protocol stack for processing the message according to a particular protocol stack, wherein the message is a data packet comprising

a sender address specifying the address of the terminal,

a port number specifying the application address of the instance sending the message at the terminal, and

user data including the contents of the message, and the server further comprising:

license control means for controlling the access right of the message to enter the server before the message is allowed to pass to the protocol stack, characterised in that the server further comprises

connection means for establishing a session between the server and the terminal and for receiving the data packet within the session,

storage means for storing a number of access right licenses purchased by a licensee, and

means for reserving a license of the licensee for each data packet arriving in a new concurrent session relating to the licensee, and

means for controlling that the number of reserved licenses does not exceed the number of purchased access right licenses.

In one particular embodiment, the invention comprises a gateway server serving a plurality of mobile terminals. It may be a WAP gateway. For example, commands, such as WAP requests, may be sent in short messages (generated by SMS) and sent to a WAP/HTTP gateway. The gateway will interpret these as WAP network packets and will perform the necessary HTTP transactions on an origin server. After that it sends back a WAP message on the same bearer, i.e. as an SMS message containing the result.

According to a second aspect of the invention there is provided a method of controlling, at a server, access right of a message received from a terminal at the server, and where the message is processed by a protocol stack, and where the message is a data packet comprising

a sender address specifying the address of the terminal,

a port number specifying the application address of the instance sending the message at the terminal, and

user data including the contents of the message,

and the method comprising:

checking the right of the message to enter the server before the message is allowed to pass to the protocol stack, characterised in that the method further comprises:

establishing a session between the server and the terminal and for receiving the data packet within the session,

and the checking of the right of the message to enter the server comprises the steps of:

storing a number of access right licenses purchased by a licensee, and

reserving a license of the licensee if the data packet arrived in a new concurrent session relating to the licensee, and

controlling that the number of reserved licenses does not exceed the number of purchased access right licenses.

According to a third aspect of the invention there is provided a computer program product for controlling, at a server, access right of a message received from a terminal at the server, where the message is processed by a protocol stack and wherein the message is a data packet comprising

a sender address specifying the address of the terminal,

a port number specifying the application address of the instance sending the message at the terminal, and

user data including the contents of the message,

and the computer program product comprising:

computer readable program means for controlling the access right of the message to enter the server before the message is allowed to pass to the protocol stack, characterised in that the computer program product further comprises

computer readable program means for causing the server to establish a session between the server and the terminal and for receiving the data packet within the session,

computer readable program means for causing the server to store a number of access right licenses purchased by a licensee, and

computer readable program means for causing the server to reserve a license of the licensee for each data packet arriving in a new concurrent session relating to the licensee, and

computer readable program means for causing the server to control that the number of reserved licenses does not exceed the number of purchased access right licenses.

Preferably the invention is implemented as software, which when loaded into a computer will function as a gateway server according to the present invention.

The invention will be discussed below in detail by referring to the enclosed drawings, in which

Figure 1 shows an arrangement of protocol stacks in the Wireless Application Protocol (WAP),

Figure 2 shows a communication system,

Figure 3 shows a gateway server embodied in hardware,

Figure 4 shows a functional block diagram of a gateway server according to the present invention,and

Figure 5 shows steps performed at license control as a flow diagram.

In the following example, communication is described with reference to the Wireless Application Protocol (WAP) mentioned above. It should be noted that the invention is not limited to the use of WAP and other protocols and specifications may be used.

Figure 2 shows a communication system comprising a plurality of mobile terminals 2 having access to the Internet 4. The mobile terminals transmit signals 6 which are received by and transmitted through a wireless network 8. The wireless network can be a number of different network systems such as GSM, CDMA IS-95, TDMA IS-136, and UMTS, and can use different type of communication within one and the same system, for example SMS, GPRS or HSCSD communication within GSM. Accordingly a number of different bearers can be used for transmitting signals 6. WAP requests 6 received by the network 8 are routed to a proxy or gateway server 12. The server 12 translates WAP requests into HTTP requests and thus allows the mobile terminals 2 to request information from a web server 14 and thus browse the Internet 4. Information obtained from the web server 14 is encoded by the proxy into a suitable format and then transmitted by the wireless network to the mobile terminal 2 which requested it. The response comprises wireless mark-up language (WML) according to WAP. WML is a tag-based display language providing navigational support, data input, hyperlinks, text and image presentation, and forms. It is a browsing language similar to HMTL. The mobile terminal 2 processes and uses the information. If the web server 14 provides content in WAP/WML format, the server 12 can retrieve such content directly from the web server 14. However, if the web server provides content in WWW format (such as HTML), a filter may be used to translate the content from WWW format to WAP/WML format.

The Wireless Application Protocol is applicable to a number of different systems including GSM-900, GSM-1800, GSM-1900, CDMA IS-95, TDMA IS-136, wide-band IS-95 and third generation systems such as IMT-2000, UMTS and W-CDMA.

Although Figure 2 shows information being obtained from the Internet, the proxy itself may contain the desired information. For example, the client may retrieve information from the file system of the proxy.

In addition to the web server 14, the mobile terminals may communicate with a wireless telephony application (WTA) server 18.

Figure 3 shows a gateway server embodied in hardware such as a computer 20. The computer 20 has dynamic memory, processing power and memory to store all of the programs needed to implement the gateway server such as the application program, the protocol stacks and the operating system. The computer 20 comprises a user interface such as a keyboard 22 and a display 23 and a server program 24. The server program 24 has an application program 26 for processing events of the underlying protocol, such as handling a request to retrieve WML from a server, and protocol stacks such as a WAP protocol stack 28 and a HTTP protocol stack 30. The application program 26 controls flow of data, including commands, requests and information, between the computer and various networks including a telephone network 32, the Internet 34 and a data network and circuit switched data networks 35. The application program 26 may further run a program that can be seen on the display 23 and controlled with the keypad 22 (and e.g. a mouse). The computer 20 communicates with the Internet 34 through the HTTP protocol stack 30 and an interface 36. The computer 20 communicates with the telephone network 34 and the data network 35 through interfaces 38 and 40. The server program 24 also comprises a gateway 42 which converts between HTTP and WAP. SMS messaging may be provided via a data connection through appropriate hardware to the operator's network.

Individual threads 44 present in the application program 26 and the WAP protocol stack 28 use processors 46 in the computer 20 to carry out necessary processing tasks. Allocation of threads to processors is provided by threading services 48 present within the operating system 50 of the computer 20.

As shown in Figure 1 the WAP stack is built on top of so called bearers (which provide datagram services). These bearers can be, for example, SMS or CSD. The bearers have their own protocol and are implemented through protocol stack implementations.

Figure 4 shows a functional block diagram (embodied in software) of a gateway server hierarchy according to the present invention, at least to the extent for understanding the invention. The gateway server includes a Wireless Protocol Stack (WPS) 50, such as the WAP stack shown in Figure 1. Below the WPS are the different bearer adapters 51 which access the different bearers through bearer drivers 52.

The function of a bearer adapter has been specified in the Wireless Datagram Protocol specification, i.e. the WDP specification of WAP. There the bearer adapter is called an Adaptation Layer or Tunnel. The Adaptation Layer is the layer of the WDP protocol that maps the WDP protocol functions directly onto a specific bearer. The Adaptation Layer is different for each bearer and deals with the specific capabilities and characteristics of that bearer service. Moreover, at the WAP Gateway or server the Tunnel terminates and passes the WDP packets on to a WAP Proxy/Server via a Tunnelling protocol, which is the interface between the Gateway that supports the bearer service and the WAP Proxy/Server.

The Adaptation Layer or Bearer Adapter is thus a component that connects the WAP Server to the wireless network. To support a number of different bearers the gateway server will thus need to have a number of different bearer adapters 51.

All data from a WAP terminal comes to the gateway server via a bearer represented in the figure by bearer drivers 52 and bearer adapters 51. From the bearer adapter the data enters the WAP stack 50, which can include all or only some of the protocol layers shown in Figure 1. According to the present invention it has been realised to perform license control directly from the data entering the gateway before it enters the protocol stack 50. In order to do this there is provided functionally between the WPS 50 and the bearer adapters 51 a bearer gate 53, through which all datagram traffic between a bearer adapter and the WPS passes. Accordingly the bearer gate 53 performs the license control, i.e. checks if every incoming data packet has access rights or not, whereby the packet is either allowed to pass to the protocol stack for processing or is discarded.

The WDP specification specifies a service primitive T-DUnitdata used to transmit data. It comprises amongst other the following parameters:

1) The *Source Address*, which is the address of the sender and is the unique address of the device making a request to the WDP layer. The source address may be an MSISDN number (Mobile Station ISDN number), IP address (given as numbers e.g. 153.226.0.56 or as symbols a.g. mycomputer.company.subsidiary.com), X.25 address or other identifier. Thereby the length of the Source Address parameter may vary according to what the source is.

2) The *Source Port*, which is the application address or port number associated with the source address of the requesting communication instance. The port number of the sender is a 16-bit number.

3) The *User Data* , which is the user data carried by the WDP protocol. The unit of data submitted to or received from the WDP layer is also referred to as the Service Data Unit. This is the complete unit (message, packet, package) of data which the higher layer (at the sender) has submitted to the WDP layer for transmission. The WDP layer will transmit the Service Data Unit and deliver it to its destination without any manipulation of its content.

The *Source Address* and *Source Port* parameters are part of a header portion of a WAP message and the *User Data* is the actual payload or data of the message.

For license control the bearer gate will read both the *Source Address* and *Source Port* information in every data packet that is received at the bearer gate 53 via the bearer adapters 51. Each combination of a client address (*Source Address*) and a client port (*Source Port*) makes up a concurrent session and thereby requires one license. This means that the same terminal can consume more than one license, for example if the user is concurrently using two different applications at the terminal by accessing a service via the gateway server (e.g. a banking application and a calendar application). Usage of also the client port number (*Source Port*) for identifying the sender is necessary to prevent someone from using a proxy machine to circumvent the license check (with UDP bearer), in which case several terminals could go via the proxy machine to the gateway, whereby the *Source Address* would always be the same. However, the *Source Port* information in the data packet would still be different.

The licenses are calculated on a session basis, i.e. controlling concurrent sessions from the same license source. There is no limit for number of transactions, but the license control is about how many sessions are allowed to execute transactions concurrently. Preferably in an embodiment of the present a fixed size time window has been provided during a session needs a license to execute transactions. The time window may be for example 10 minutes. This means that when a session is established one license is reserved (which is done for every combination of *Source Address* and *Source Port)*. If no data arrives to the gateway server over that session during that time window, i.e. during 10 minutes, the license is released. Next time that session wants to execute a transaction, a new license is needed, i.e. that data in that session is allowed to pass only if there still is a free license for that license holder.

The idea of the time window in the licensing check is that gateway server accepts during the last 10 minutes data packets only from Y different concurrent sessions. If a data packet from a concurrent session Y+1 is received, Wireless Control

Message Protocol (WCMP) message 'Destination Unreachable (address unreachable)' is sent to the client (i.e to the WAP terminal).

The maximum number of the concurrent sessions, Y, is determined by checking the contents of a license storage file (that is stored in a server computer in a normal manner) when the server is started. The license storage file contains encrypted license strings. Each license string allows a certain number concurrent sessions, e.g. 5/10/30/100 or 1000 additional concurrent sessions.

The steps performed at the bearer gate for checking the access rights of a data packet is described in following in relation to Figure 5. At step 60 a data packet is received at the bearer gate via a bearer adapter. At step 61 the address and port number of the sender is read from the data packet. The bearer gate handles the remote address (*Source Address*) as unformatted binary data undependent of whether it is an MSISDN, IP address, X.25 address or other identifier. At step 62 the current time T is attached to the message. For this purpose the server keeps a clock as is normal for computers. Next, at step 63 a check is being made from a list or file of already reserved licenses to see if any reservation or entry is older than the allowed time window, which in this example is 10 minutes. If such an entry is found, the entry is removed from the list or file and the license is freed. Also at step the number of entries in use C, i.e. the number of the licenses in use, is counted. At step 64 a check is made to see if a license already exists for the session in which the data packet was received (i.e if less than 10 minutes has passed since the last transaction in that session). If 'yes', the time in the entry is updated in the entry file and processing of the data packet is allowed, whereby the data packet is allowed to pass to the protocol stack (step 65). If the answer to the check at step 64 is 'no', the question is about a new concurrent session, in which case we go to step 66.

In step 66 it is checked whether the number of licenses C in use by the particular licensee is less than the number of licenses Y that the licensee has purchased. If 'yes', goto step 67 where a new license is taken into use, i.e. a new entry is marked to the entry list, C is incremented by one and processing of the message

is allowed, whereby the data packet is allowed to pass to the protocol stack. If the answer to step 66 is 'no', whereby the number of licenses C in use by the particular licensee is equal to (or more which it shouldn't be) than the number of licenses Y that the licensee has purchased, a WCMP message (Wireless Control Message Protocol) with the contents "Destination Unreachable" is sent by the bearer gate to the client terminal, and the data packet is discarded (step 68). Relating to step 66, the maximum number of concurrent sessions, i.e. the number of licenses that the license holder has purchased, Y, is determined by checking the contents of the license storage list (e.g. a separete file) when the server is started. The license storage file contains encrypted license strings. Each license string allows e.g. 5/10/30/100 or 1000 additional concurrent sessions.

If it is assumed that all data packets have come from a known and valid client address, then the above explained steps are sufficient for performing the license control. This can be a good approach for the purposes of controlling that the service provider does not exceed the number of licenses purchased from the manufacturer of the gateway server. However, a service provider might want to restrict access to messages coming only from certain predetermined terminals. For that purpose a separate check might be made by keeping at the gateway server a list (or separate file) of allowed addresses and port numbers in general and related to a particular license, whereby if the address and port number do not correspond to any allowed license then the message is discarded and an error message is returned. That check can be done fully separately from the license control check of Figure 5 is performed of after step 61 in Figure 5.

Returning to Figure 4 the bearer gate 53 has a link to a server manager 54, which controls server operation. The server manager 54 gets control commands from the administrator 55, who is allowed to control server operation with a user interface 56, such as the keypad 22 and display 23 shown in Figure 3. The connection to Internet, such as to a web server is via interface 57.

Between the bearer gate 53 and WPS 50 there is an interface 58a, which is an interface to send and receive WDP datagrams and to retrieve information about

the Bearer adapter 51. Further the datagrams are transferred between the bearer gate and the bearer adapter over interface 58b. There is further an interface 59 between the server manager 54 and bearer gate 53 for controlling and configuring the operation of the server and bearer gate 53. Via the user interface 56 the number of licenses purchased or held by a licensee can be changed by the administrator 55.

The different operations and functional blocks shown in Figure 4 are preferably implemented as software blocks, which are run by processor 46 by calling threads 44 in the application program 26 and protocol stack 28.

The present invention discloses a method by which license control can be handled in a simple manner by performing it below the protocol stack (in view of the server hierarchy). In a WAP gateway server any requirement of using many separate license systems for all combinations of the WAP protocol are avoided by the present invention. A license control system could also be implemented above or within the WAP stack, but would lead to separate license control systems for different protocol combinations. The remote client, i.e. the terminal can make a connection to the WAP server using any of the layers or using many combinations of the protocols. For example, looking at Figure 1, protocol combinations WDP+WTLS (for services that only require datagram transport with security) , WDP+WTP (for applications that only require transaction services without security), WDP+WTP+WSP (for applications that do not require security, but otherwise normal WAP sessions), WDP+WTLS+WTP (for applications that only require transaction services with security) and WDP+WTLS+WTP+WSP (full WAP stack) are all possible and they would all need own licensing counting system, if implemented above the stack. If license control would be implemented above or within the WAP stack, also the problem that not all protocols do use sessions at all, would arise and would need to be solved. For example implementing a licensing system that limits the maximum number of concurrent WSP sessions is easy, but there is also connectionlesss WSP protocol that does not use sessions at all. The present invention, by checking the remote address and remote port

information below the protocol stack in every data packet solves this problem in a general way.

The invention can be implemented as software, which when loaded into a computer will function as a gateway server according to the present invention. The functionality of the license control according to the invention can be programmed e.g. in the C or Java programming language, or any other programming language.

This paper presents the implementation and embodiments of the invention with the help of examples. It is obvious to a person skilled in the art, that the invention is not restricted to details of the embodiments presented above, and that the invention can be implemented in another embodiment without deviating from the characteristics of the invention. For example, although the foregoing is a related to mobile terminals browsing the Internet or a WAP proxy, it is to be understood that the communication may be of different types including sending and receiving information, conducting transactions such as financial transactions sending and receiving electronic mail or messages. The range of activities includes accessing services, for example weather reports, news, stock prices, flight schedules, downloading ringing tones, banking services including information provision and payments. It may occur in communications environments other than the Internet and may also be used with other protocol stacks than WAP. Thus, the presented embodiments should be considered illustrative, but not restricting. Hence, the possibilities of implementing and using the invention are only restricted by the enclosed patent claims. Consequently, the various options of implementing the invention as determined by the claims, including the equivalent implementations, also belong to the scope of the present invention.

Claims

1. A method of controlling, at a server, access right of a message received from a terminal at the server, and where the message is processed by a protocol stack (50), and where the message is a data packet comprising

a sender address specifying the address of the terminal,

a port number specifying the application address of the instance sending the message at the terminal, and

user data including the contents of the message,

and the method comprising:

checking the right of the message to enter the server before the message is allowed to pass to the protocol stack (50), **characterised** in that the method further comprises:

establishing a session between the server and the terminal and for receiving the data packet within the session,

and the checking of the right of the message to enter the server comprises the steps of:

storing a number (Y) of access right licenses purchased by a licensee, and

reserving a license (C) of the licensee if the data packet arrived in a new concurrent session relating to the licensee, and

controlling that the number of reserved licenses (C) does not exceed the number of purchased access right licenses (Y).

2. A method according to claim 1, **characterised** in that the method further comprises

reading both the sender address and the port number from the data packet for identifying the terminal.

3. A method according to claim 1, **characterised** in that the method further comprises:

communicating messages with a particular wireless network and adapting messages received from the wireless network for the protocol stack (50), and after the adaptation performing the steps of checking the access right.

4. A method according to claim 1, **characterised** in that the method further comprises:

reserving a license for the session as a response to having determined existance of access right, and

monitoring the time passed since the last data packet arrived in one session, and releasing the license for the session where a predetermined time has passed since the last data packet arrived in the session.

5. A method according to claim 2, **characterised** in that the method further comprises:

reserving a license (C) for each different combination of sender address and port number found in a data packet.

6. A method according to claim 1, **characterised** in that the method further comprises:

passing the message to the protocol stack (50) in response to determining allowed access, and

discarding the message in response to determining denied access.

7. A method according to claim 6, **characterised** in that the method further comprises:

returning an error message to the terminal in response to a discarded message.

8. A method according to claim 4, **characterised** in that where the license has been released for a particular session and a data packet again arrives in that session, performing the access right checking for the newly received data packet and reserving a new license upon allowed access.

9. A method according to claim 4, **characterised** in that where a data packet arrives before said predetermined time has passed, performing the access right

checking for the newly received data packet, and allowing access on basis of the already reserved license without reserving a new license.

10. A method according to any preceding claim, **characterised** in that the terminals comprise mobile terminals, for example cellular telephones, supporting the Wireless Application Protocol, WAP.

11. A server for receiving a message from a terminal and comprising a protocol stack (50) for processing the message according to a particular protocol stack, wherein the message is a data packet comprising

a sender address specifying the address of the terminal,

a port number specifying the application address of the instance sending the message at the terminal, and

user data including the contents of the message, and the server further comprising:

license control means (53) for controlling the access right of the message to enter the server before the message is allowed to pass to the protocol stack (50), **characterised** in that the server further comprises

connection means (50 - 52) for establishing a session between the server and the terminal and for receiving the data packet within the session,

storage means for storing a number (Y) of access right licenses purchased by a licensee, and

means for reserving a license (C) of the licensee for each data packet arriving in a new concurrent session relating to the licensee, and

means for controlling that the number of reserved licenses (C) does not exceed the number of purchased access right licenses (Y).

12. A server according to claim 11, **characterised** in that the server further comprises

means (53) for reading both the sender address and the port number from the data packet for identifying the terminal.

13. A server according to claim 11, **characterised** in that the server further comprises

a bearer adapter (51) for communicating messages with a particular wireless network and for adapting messages received from the wireless network for the protocol stack (50), and wherein the license control means (53) have been placed functionally below the protocol stack (50) and above the bearer adapter (51) in the server hierarchy.

14. A server according to claim 12, **characterised** in that the server further comprises

reservation means (53) for reserving a license for the session as a response to the license control means (53) having determined existance of access right, and

timing means (53) for monitoring the time passed since the last data packet arrived in one session, and releasing the license for the session where a predetermined time has passed since the last data packet arrived in the session.

15. A server according to claim 12, **characterised** in that the server further comprises

means for reserving a license (C) for each different combination of sender address and port number found in a data packet.

16. A server according to claim 11, **characterised** in that server further comprises means (53) for passing the message to the protocol stack (50) in response to determining allowed access and for discarding the message in response to determining denied access.

17. A server according to claim 16, **characterised** in that server further comprises means (53) for returning an error message to the terminal in response to a discarded message.

18. A server according to any of claims 11-17, **characterised** in that the server comprises a gateway server serving a plurality of mobile terminals.

19. A server according to claim 18, **characterised** in that the server comprises a Wireless Application Protocol, WAP, gateway.

20. A computer program product for controlling, at a server, access right of a message received from a terminal at the server, where the message is processed by a protocol stack (50) and wherein the message is a data packet comprising

a sender address specifying the address of the terminal,

a port number specifying the application address of the instance sending the message at the terminal, and

user data including the contents of the message,

and the computer program product comprising:

computer readable program means (53, 56, 63) for controlling the access right of the message to enter the server before the message is allowed to pass to the protocol stack (50), **characterised** in that the computer program product further comprises

computer readable program means for causing the server to establish a session between the server and the terminal and for receiving the data packet within the session,

computer readable program means for causing the server to store a number (Y) of access right licenses purchased by a licensee, and

computer readable program means for causing the server to reserve a license (C) of the licensee for each data packet arriving in a new concurrent session relating to the licensee, and

computer readable program means for causing the server to control that the number of reserved licenses (C) does not exceed the number of purchased access right licenses (Y).

Martin Raepple
E-Mail: mraepple@vnet.ibm.com

Lektorat: Dr. Michael Barabas
Satz: FrameMaker-Dateien des Autors
Copy-Editing: Heike Pich, München
Herstellung: Josef Hegele
Umschlaggestaltung: Helmut Kraus, Düsseldorf
Druck: Koninklijke Wöhrmann B.V., Zutphen, Niederlande

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Raepple, Martin:
Sicherheitskonzepte für das Internet : Grundlagen, Technologien und Lösungskonzepte für die kommerzielle Nutzung / Martin Raepple.
1. Aufl. – Heidelberg : dpunkt-Verl., 1998
ISBN 3-932588-14-2

1. Auflage 1998
Copyright © 1998 dpunkt – Verlag für digitale Technologie GmbH
Ringstraße 19
69115 Heidelberg

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Alle Informationen in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

In diesem Buch werden eingetragene Warenzeichen, Handelsnamen und Gebrauchsnamen verwendet. Auch wenn diese nicht als solche gekennzeichnet sind, gelten die entsprechenden Schutzbestimmungen.

Das verwendete Papier ist aus chlorfrei gebleichten Rohstoffen hergestellt und alterungsbeständig.

5 4 3 2 1 0

Vorwo

Das Internet
mente im W
Potential ers
Marketing-
kanal. Entsc
keiten ist ab
ter in diesem
Vertrauensge
Marktplatz‹.
oder Verträg
voraus, das
gegeben ist.
scheint diese
auf dem Weg

In der St
häufig nur un
Mit steigende
Dienste komn
Bedeutung zu
wirkungsvolle
alleine durch
Problem beso
lichen Lösung
heitskonzept,
dungen im Int
Verzahnung m
men berücksic
nischen Aspek

Die Umset
mals nicht nu
sicherheitsrelev
trauens- und
gravierendere F
Der Aufwand v

Die Hauptaufgabe einer Firewall ist es, die Zugriffskontrolle auf das interne Netzwerk zu zentralisieren. Aus diesem Grund kann das System das Unternehmen nur so gut oder schlecht vor Angriffen schützen, wie alternative Verbindungswege zum Internet durch eine entsprechend formulierte und praktizierte Sicherheitspolitik unterbunden werden. Ein Mitarbeiter, der sich vom Arbeitsplatz aus über ein Modem bei seinem privaten Service Provider einwählt, öffnet unter Umgehung der Firewall Tür und Tor für externe Angreifer. Die Konzentration des Übergangs zwischen dem internen und externen Netz auf ein einziges System ermöglicht es auf einfache Weise, neben Zugriffs- und Auditmechanismen noch weitere Sicherheitskontrollen zentral zu implementieren. Viele Hersteller von Firewallsystemen haben dies erkannt und erweitern ihre Produkte um zusätzliche Funktionen, wie z. B. automatischer Virencheck von FTP-Downloads und E-Mail-Attachments (siehe 2.11).

Zentralisierung des Internetzugriffs

Technisch gesehen existieren zwei verschiedene Konzepte, nach denen Firewalls realisiert werden: Paketfilter und Proxy Gateways. Sie unterscheiden sich im wesentlichen durch die Protokollebene, auf der die Zugriffskontrollen wirksam sind, und ob die Verbindungen durch die Firewall unverändert weitergeleitet oder getrennt werden. Je weiter oben die Firewall im Schichtenmodell angesiedelt ist, desto höher ist ihre Schutzwirkung. In der Praxis gibt es häufig keine Standardlösung. Statt dessen kommt eine Kombination der verschiedenen Ansätze zum Einsatz (siehe 3.3). Wie in einer Bank ergänzen sich die unterschiedlichen Zugangskontrollen, ohne dabei die Geschäftstätigkeit zu behindern. Videokameras überwachen passiv die Eingangsbereiche und beobachten jeden ein- und ausgehenden Kunden. Die öffentlichen Schalter werden von den internen Büroräumen durch Türen getrennt, und die Ersparnisse der Kunden lagern hinter dicken Tresorwänden, die nur von autorisierten Mitarbeitern und mit der richtigen Zahlenkombination geöffnet werden können.

Zugriffskontrolle auf unterschiedlichen Ebenen

2.6.1 Paketfilter

Paketfilter oder Überwachungsrouter (engl. screening router) arbeiten auf der Netzwerkschicht und stellen die einfachste Variante einer Firewall dar. Sie können ein- und ausgehende Datenpakete nach den Informationen in den Headern von IP, ICMP, TCP und UDP auswerten. In der Regel sind das die Sende- und Empfangsadresse, die Portnummer der Anwendung, TCP-Statusinformationen (Flag-Bits, siehe Anhang A.5) sowie der Nachrichtentyp bei ICMP-Paketen (siehe 1.9.2 und Anhang A.6).

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 January 2001 (11.01.2001)

PCT

(10) International Publication Number
WO 01/03368 A1

(51) International Patent Classification[7]: H04L 12/00

(21) International Application Number: PCT/FI00/00513

(22) International Filing Date: 7 June 2000 (07.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
991493 30 June 1999 (30.06.1999) FI

(71) Applicant *(for all designated States except US)*: NOKIA CORPORATION [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: SOLALA, Erkki [FI/FI]; Halimajärventie 53, FIN-36100 Kangasala as (FI).

(74) Agent: JOHANSSON, Folke; Nokia Corporation, P.O. Box 319, FIN-00045 Nokia Group (FI).

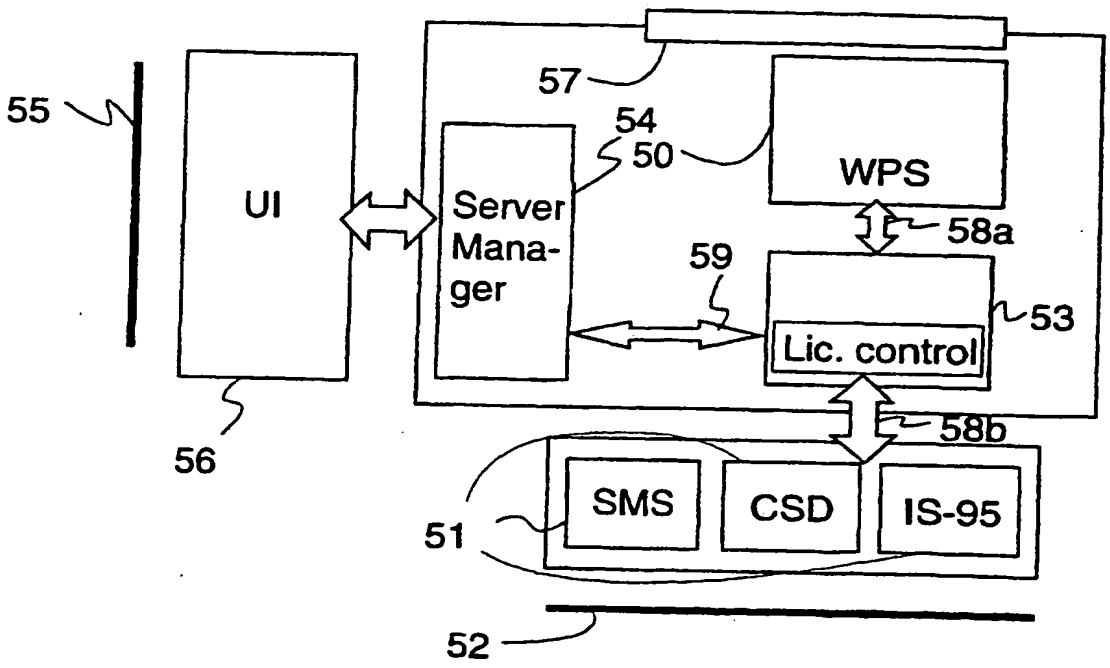
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AT (utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: LICENSE CONTROL AT A GATEWAY SERVER



(57) Abstract: The invention relates to a gateway server for receiving a message from a terminal and comprising a protocol stack (50) for processing the message according to a particular protocol stack. The server further comprises license control means (53) for controlling the access right of the message to enter the server before the message is allowed to pass to the protocol stack (50). The invention also relates to a method and a computer program product for controlling, at a server, access right of a message received from a terminal at the server.

WO 01/03368 A1

— *Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

License control at a gateway server

The present invention relates to license control at a gateway server for controlling the right for a message to enter the server. It is particularly suitable for a mobile protocol such as WAP (Wireless Application Protocol) for enabling a mobile terminal to access the Internet via the gateway server.

The term "Internet" is commonly used to describe information, content, which can be accessed using a terminal, typically a PC, connected via a modem to a telecommunications network. The content can be stored at many different sites remote from the accessing computer, although each of the remote sites is also linked to the telecommunications network. The content can be structured using HyperText Mark-up Language (HTML). The Internet is made workable by the specification of a standard communications system which makes use of a number of protocols, such as the Transfer Control Protocol (TCP), the User Datagram Protocol (UDP), and the Internet Protocol (IP), to control the flow of data around the numerous different components of the Internet. TCP and UDP are concerned with the prevention and correction of errors in transmitted Internet data. IP is concerned with the structuring and routing of data. On top of that, other application specific protocols may be provided to manage and manipulate the various kinds of information available via the Internet, for example HTTP to access HTML content, FTP to access files or SMTP to access e-mail.

The Internet is physically constructed from a hierarchy of telecommunication and data communication networks, for example local area networks (LANs), regional telephone networks, and international telephone networks. These networks are connected internally and externally by so-called "routers" which receive data from a source host, or a previous router in a transmission chain, and route it to the destination host or the next router in the transmission chain.

With increased use of mobile cellular telephones, there is a growing demand for so-called mobile Internet access, in which access is made from a portable

computer connected to a cellular telephone or from an integrated computer/cellular phone device. Typically, the purpose of such access is to obtain content from the Internet. It has also been proposed to provide Internet access to advanced mobile terminals, so-called communicators and smart phones, by means of the Wireless Application Protocol (WAP), for example. WAP has an architecture in which there is a protocol stack having an application layer (called the Wireless Application Environment or WAE), a session layer (called the Wireless Session Protocol or WSP), a transaction layer (called the Wireless Transaction Protocol or WTP), a security layer (called Wireless Transport Layer Security or WTLS) and a transport layer (called the Wireless Datagram Protocol or WDP) as shown in Figure 1. Each of the layers of the architecture is accessible by the layers above as well as by other services and applications. These protocols are designed to operate over a variety of different bearer services such as SMS (Short Message Service), CSD (Circuit Switched Data), GPRS (General Packet Radio Service) etc. A specification describing the WAP architecture and the protocol layers is available from http//www.wapforum.org/.

Obtaining access to the Internet generally involves having sessions between a terminal, such as a mobile terminal, and a server. A session is a series of interactions between a terminal and a server having a well-defined beginning and end and involving agreed-upon characteristics. Typically, a session involves a peer announcing to another peer a desire to establish a session, both peers negotiating the characteristics of the session, the peers engaging in a variety of transactions and one of the peers ending the session. The characteristics which are negotiated are typically the length of packets to be exchanged, the character sets which can be understood and manipulated and the versions of protocols which are to be used. A transaction is a basic unit of interaction and may include requesting and receiving information, aborting an ongoing session and informing a peer of a situation in an on-going session. All session operations to establish and terminate a session as well as all transactions result in events being generated and received by the peer. There are many event sources (sessions and transactions).

The operations which an application can invoke to generate events are called service primitives. Service primitives represent the logical exchange of information and control between the session layer and other layers. They consist of commands and their respective responses associated with the particular service provided. Invoking a service primitive in a peer on one side of a communication link results in an event being generated in a peer in the other side of the link. Service primitives are present in all communication protocols.

An active session can involve multiple transactions and so can generate multiple events. Depending on the speed at which an application can process events coming from its peer, it can happen that there are more transactions than it can process and so it receives more events than it can process. In this case, the events are queued up and wait to be processed within the context of that session. Events connected or related to the same session generally need to be processed in a specific order. In some protocols, a session can be suspended, in which state no transactions are allowed except a request to resume or to terminate.

In WAP, communication between layers and between entities within the session layer are also accomplished by means of service primitives.

Most transactions are either of the push type or of the pull (request-reply) type. In push type transactions a peer sends information which has not been specifically requested and in pull type transactions, a peer specifically requests to receive information from another peer.

Terminals, such as personal computers, obtain information from the Internet through a server, such as a gateway server. The Internet uses HTTP which is a simple request-reply protocol. Almost the only event is an HTTP request. The operating system of the server runs a number of applications and so creates a number of threads to deal with them, for example proxies and mail servers. The applications use the available threads as they are required. In the case of Internet

access by a PC, it is convenient to create a thread in the server dynamically to deal with each request because the requests are independent from each other. Once the request has been processed, the thread has finished its activity and is terminated.

In a communication system comprising a gateway server and a plurality of mobile terminals, establishing a session requires a relatively large amount of bandwidth because a terminal and a server must negotiate many characteristics relevant to the session. Furthermore, information which is unique to a particular opened session may be lost if the session is terminated. This unique information could have been negotiated as a result of transactions. For example, it may be the status of a game. In order to avoid opening and closing sessions on demand and establishing new sessions whenever they are needed, the sessions may be kept open for a long time, even in an inactive state, so that they can be resumed when needed. A session can remain open for days or even weeks until it is closed or until the terminal no longer receives power, for example from a battery. An application in the server will use the operating system thread management service and create a number of threads to manage these sessions.

In WAP typically a gateway server will be the port for allowing a terminal to access the Internet. The gateway server will be provided by e.g. a service provider, and users may access the gateway server by purchasing a license or number of licenses from the service provider. Accordingly, there is a need to implement a solution at the gateway server for controlling access to the gateway server. Equally the gateway server is usually implemented as a computer program which when loaded into a computer works as a gateway server. Thereby the manufacturer of the gateway server, i.e. the maker of the computer program, may sell licenses to the service provider, which limits the number of users that the service provider is able to serve without purchasing additional licenses from the manufacturer. Thus there is a need to implement a solution at the gateway server for controlling number of total licenses in use at the server.

Now a gateway server has been invented where license control is performed on a message entering the gateway server before it is allowed to pass on to the protocol stack, i.e. license control is performed below the protocol stack in the gateway server hierarchy. Identification of the sender of the message is checked to determine access rights. In a WAP gateway or proxy server there is more specifically provided below the WAP stack and above the bearers a bearer gate which performs the license control, and through which all data traffic coming from the bearers passes before going to the protocol stack.

The present invention can be used for controlling access right of a message in both of the above mentioned situations, namely for controlling that the service provider does not exceed the number of licenses it has purchased from the manufacturer of the gateway server and for controlling that a user entity having purchased a number of licenses from the service provider does not exceed that number of licenses.

In a preferred embodiment of the invention datagrams or data packets are received via a particular bearer. This data packet has an address of the sender, also called source address, remote address or client address. Moreover, each data packet has a port number of the sender, also called source port, remote port or client port information. In an embodiment of the present invention both the address and port number of the sender are checked for identifying the sender for license control purposes.

Licenses are calculated on a session basis, i.e. controlling concurrent sessions from the same license holder. There is no limit for number of transactions that are allowed during a session per license, but the license control is about how many sessions are allowed to execute transactions concurrently. In a particular embodiment the sessions will be given a time window during which the license is reserved, and unless there is data traffic within that session within the time window, the license for that session will be released. Next time there is a need for

executing transactions within that session, a new license needs to be taken into use.

According to a first aspect of the invention there is provided a server for receiving a message from a terminal and comprising a protocol stack for processing the message according to a particular protocol stack, the server further comprising: license control means for controlling the access right of the message to enter the server before the message is allowed to pass to the protocol stack.

In one particular embodiment, the invention comprises a gateway server serving a plurality of mobile terminals. It may be a WAP gateway. For example, commands, such as WAP requests, may be sent in short messages (generated by SMS) and sent to a WAP/HTTP gateway. The gateway will interpret these as WAP network packets and will perform the necessary HTTP transactions on an origin server. After that it sends back a WAP message on the same bearer, i.e. as an SMS message containing the result.

According to a second aspect of the invention there is provided a method of controlling, at a server, access right of a message received from a terminal at the server, and where the message is processed by a protocol stack, the method comprising:
checking the right of the message to enter the server before the message is allowed to pass to the protocol stack.

According to a third aspect of the invention there is provided a computer program product for controlling, at a server, access right of a message received from a terminal at the server, and where the message is processed by a protocol stack, the computer program product comprising:
computer readable program means for controlling the access right of the message to enter the server before the message is allowed to pass to the protocol stack.

Preferably the invention is implemented as software, which when loaded into a computer will function as a gateway server according to the present invention.

The invention will be discussed below in detail by referring to the enclosed drawings, in which

Figure 1 shows an arrangement of protocol stacks in the Wireless Application Protocol (WAP),

Figure 2 shows a communication system,

Figure 3 shows a gateway server embodied in hardware,

Figure 4 shows a functional block diagram of a gateway server according to the present invention,and

Figure 5 shows steps performed at license control as a flow diagram.

In the following example, communication is described with reference to the Wireless Application Protocol (WAP) mentioned above. It should be noted that the invention is not limited to the use of WAP and other protocols and specifications may be used.

Figure 2 shows a communication system comprising a plurality of mobile terminals 2 having access to the Internet 4. The mobile terminals transmit signals 6 which are received by and transmitted through a wireless network 8. The wireless network can be a number of different network systems such as GSM, CDMA IS-95, TDMA IS-136, and UMTS, and can use different type of communication within one and the same system, for example SMS, GPRS or HSCSD communication within GSM. Accordingly a number of different bearers can be used for transmitting signals 6. WAP requests 6 received by the network 8 are routed to a proxy or gateway server 12. The server 12 translates WAP requests into HTTP requests and thus allows the mobile terminals 2 to request information from a web server 14 and thus browse the Internet 4. Information obtained from the web server 14 is encoded by the proxy into a suitable format and then transmitted by the wireless network to the mobile terminal 2 which requested it. The response comprises wireless mark-up language (WML) according to WAP. WML is a tag-

based display language providing navigational support, data input, hyperlinks, text and image presentation, and forms. It is a browsing language similar to HMTL. The mobile terminal 2 processes and uses the information. If the web server 14 provides content in WAP/WML format, the server 12 can retrieve such content directly from the web server 14. However, if the web server provides content in WWW format (such as HTML), a filter may be used to translate the content from WWW format to WAP/WML format.

The Wireless Application Protocol is applicable to a number of different systems including GSM-900, GSM-1800, GSM-1900, CDMA IS-95, TDMA IS-136, wide-band IS-95 and third generation systems such as IMT-2000, UMTS and W-CDMA.

Although Figure 2 shows information being obtained from the Internet, the proxy itself may contain the desired information. For example, the client may retrieve information from the file system of the proxy.

In addition to the web server 14, the mobile terminals may communicate with a wireless telephony application (WTA) server 18.

Figure 3 shows a gateway server embodied in hardware such as a computer 20. The computer 20 has dynamic memory, processing power and memory to store all of the programs needed to implement the gateway server such as the application program, the protocol stacks and the operating system. The computer 20 comprises a user interface such as a keyboard 22 and a display 23 and a server program 24. The server program 24 has an application program 26 for processing events of the underlying protocol, such as handling a request to retrieve WML from a server, and protocol stacks such as a WAP protocol stack 28 and a HTTP protocol stack 30. The application program 26 controls flow of data, including commands, requests and information, between the computer and various networks including a telephone network 32, the Internet 34 and a data network and circuit switched data networks 35. The application program 26 may further run a program that can be seen on the display 23 and controlled with the keypad 22

(and e.g. a mouse). The computer 20 communicates with the Internet 34 through the HTTP protocol stack 30 and an interface 36. The computer 20 communicates with the telephone network 34 and the data network 35 through interfaces 38 and 40. The server program 24 also comprises a gateway 42 which converts between HTTP and WAP. SMS messaging may be provided via a data connection through appropriate hardware to the operator's network.

Individual threads 44 present in the application program 26 and the WAP protocol stack 28 use processors 46 in the computer 20 to carry out necessary processing tasks. Allocation of threads to processors is provided by threading services 48 present within the operating system 50 of the computer 20.

As shown in Figure 1 the WAP stack is built on top of so called bearers (which provide datagram services). These bearers can be, for example, SMS or CSD. The bearers have their own protocol and are implemented through protocol stack implementations.

Figure 4 shows a functional block diagram (embodied in software) of a gateway server hierarchy according to the present invention, at least to the extent for understanding the invention. The gateway server includes a Wireless Protocol Stack (WPS) 50, such as the WAP stack shown in Figure 1. Below the WPS are the different bearer adapters 51 which access the different bearers through bearer drivers 52.

The function of a bearer adapter has been specified in the Wireless Datagram Protocol specification, i.e. the WDP specification of WAP. There the bearer adapter is called an Adaptation Layer or Tunnel. The Adaptation Layer is the layer of the WDP protocol that maps the WDP protocol functions directly onto a specific bearer. The Adaptation Layer is different for each bearer and deals with the specific capabilities and characteristics of that bearer service. Moreover, at the WAP Gateway or server the Tunnel terminates and passes the WDP packets on to

a WAP Proxy/Server via a Tunnelling protocol, which is the interface between the Gateway that supports the bearer service and the WAP Proxy/Server.

The Adaptation Layer or Bearer Adapter is thus a component that connects the WAP Server to the wireless network. To support a number of different bearers the gateway server will thus need to have a number of different bearer adapters 51.

All data from a WAP terminal comes to the gateway server via a bearer represented in the figure by bearer drivers 52 and bearer adapters 51. From the bearer adapter the data enters the WAP stack 50, which can include all or only some of the protocol layers shown in Figure 1. According to the present invention it has been realised to perform license control directly from the data entering the gateway before it enters the protocol stack 50. In order to do this there is provided functionally between the WPS 50 and the bearer adapters 51 a bearer gate 53, through which all datagram traffic between a bearer adapter and the WPS passes. Accordingly the bearer gate 53 performs the license control, i.e. checks if every incoming data packet has access rights or not, whereby the packet is either allowed to pass to the protocol stack for processing or is discarded.

The WDP specification specifies a service primitive T-DUnitdata used to transmit data. It comprises amongst other the following parameters:

1) The *Source Address*, which is the address of the sender and is the unique address of the device making a request to the WDP layer. The source address may be an MSISDN number (Mobile Station ISDN number), IP address (given as numbers e.g. 153.226.0.56 or as symbols a.g. mycomputer.company.subsidiary.com), X.25 address or other identifier. Thereby the length of the Source Address parameter may vary according to what the source is.

2) The *Source Port*, which is the application address or port number associated with the source address of the requesting communication instance. The port number of the sender is a 16-bit number.

3) The *User Data* , which is the user data carried by the WDP protocol. The unit of data submitted to or received from the WDP layer is also referred to as the Service Data Unit. This is the complete unit (message, packet, package) of data which the higher layer (at the sender) has submitted to the WDP layer for transmission. The WDP layer will transmit the Service Data Unit and deliver it to its destination without any manipulation of its content.

The *Source Address* and *Source Port* parameters are part of a header portion of a WAP message and the *User Data* is the actual payload or data of the message.

For license control the bearer gate will read both the *Source Address* and *Source Port* information in every data packet that is received at the bearer gate 53 via the bearer adapters 51. Each combination of a client address (*Source Address*) and a client port (*Source Port*) makes up a concurrent session and thereby requires one license. This means that the same terminal can consume more than one license, for example if the user is concurrently using two different applications at the terminal by accessing a service via the gateway server (e.g. a banking application and a calendar application). Usage of also the client port number (*Source Port*) for identifying the sender is necessary to prevent someone from using a proxy machine to circumvent the license check (with UDP bearer), in which case several terminals could go via the proxy machine to the gateway, whereby the *Source Address* would always be the same. However, the *Source Port* information in the data packet would still be different.

The licenses are calculated on a session basis, i.e. controlling concurrent sessions from the same license source. There is no limit for number of transactions, but the license control is about how many sessions are allowed to execute transactions concurrently. Preferably in an embodiment of the present a fixed size time window has been provided during a session needs a license to execute transactions. The time window may be for example 10 minutes. This means that when a session is established one license is reserved (which is done for every combination of *Source Address* and *Source Port).* If no data arrives to the gateway server over

that session during that time window, i.e. during 10 minutes, the license is released. Next time that session wants to execute a transaction, a new license is needed, i.e. that data in that session is allowed to pass only if there still is a free license for that license holder.

The idea of the time window in the licensing check is that gateway server accepts during the last 10 minutes data packets only from Y different concurrent sessions. If a data packet from a concurrent session Y+1 is received, Wireless Control Message Protocol (WCMP) message 'Destination Unreachable (address unreachable)' is sent to the client (i.e to the WAP terminal).

The maximum number of the concurrent sessions, Y, is determined by checking the contents of a license storage file (that is stored in a server computer in a normal manner) when the server is started. The license storage file contains encrypted license strings. Each license string allows a certain number concurrent sessions, e.g. 5/10/30/100 or 1000 additional concurrent sessions.

The steps performed at the bearer gate for checking the access rights of a data packet is described in following in relation to Figure 5. At step 60 a data packet is received at the bearer gate via a bearer adapter. At step 61 the address and port number of the sender is read from the data packet. The bearer gate handles the remote address (*Source Address*) as unformatted binary data undependent of whether it is an MSISDN, IP address, X.25 address or other identifier. At step 62 the current time T is attached to the message. For this purpose the server keeps a clock as is normal for computers. Next, at step 63 a check is being made from a list or file of already reserved licenses to see if any reservation or entry is older than the allowed time window, which in this example is 10 minutes. If such an entry is found, the entry is removed from the list or file and the license is freed. Also at step the number of entries in use C, i.e. the number of the licenses in use, is counted. At step 64 a check is made to see if a license already exists for the session in which the data packet was received (i.e if less than 10 minutes has passed since the last transaction in that session). If 'yes', the time in the entry is updated in the entry file and processing of the data packet is allowed, whereby the

data packet is allowed to pass to the protocol stack (step 65). If the answer to the check at step 64 is 'no', the question is about a new concurrent session, in which case we go to step 66.

In step 66 it is checked whether the number of licenses C in use by the particular licensee is less than the number of licenses Y that the licensee has purchased. If 'yes', goto step 67 where a new license is taken into use, i.e. a new entry is marked to the entry list, C is incremented by one and processing of the message is allowed, whereby the data packet is allowed to pass to the protocol stack. If the answer to step 66 is 'no', whereby the number of licenses C in use by the particular licensee is equal to (or more which it shouldn't be) than the number of licenses Y that the licensee has purchased, a WCMP message (Wireless Control Message Protocol) with the contents "Destination Unreachable" is sent by the bearer gate to the client terminal, and the data packet is discarded (step 68). Relating to step 66, the maximum number of concurrent sessions, i.e. the number of licenses that the license holder has purchased, Y, is determined by checking the contents of the license storage list (e.g. a separete file) when the server is started. The license storage file contains encrypted license strings. Each license string allows e.g. 5/10/30/100 or 1000 additional concurrent sessions.

If it is assumed that all data packets have come from a known and valid client address, then the above explained steps are sufficient for performing the license control. This can be a good approach for the purposes of controlling that the service provider does not exceed the number of licenses purchased from the manufacturer of the gateway server. However, a service provider might want to restrict access to messages coming only from certain predetermined terminals. For that purpose a separate check might be made by keeping at the gateway server a list (or separate file) of allowed addresses and port numbers in general and related to a particular license, whereby if the address and port number do not correspond to any allowed license then the message is discarded and an error message is returned. That check can be done fully separately from the license control check of Figure 5 is performed of after step 61 in Figure 5.

Returning to Figure 4 the bearer gate 53 has a link to a server manager 54, which controls server operation. The server manager 54 gets control commands from the administrator 55, who is allowed to control server operation with a user interface 56, such as the keypad 22 and display 23 shown in Figure 3. The connection to Internet, such as to a web server is via interface 57.

Between the bearer gate 53 and WPS 50 there is an interface 58a, which is an interface to send and receive WDP datagrams and to retrieve information about the Bearer adapter 51. Further the datagrams are transferred between the bearer gate and the bearer adapter over interface 58b. There is further an interface 59 between the server manager 54 and bearer gate 53 for controlling and configuring the operation of the server and bearer gate 53. Via the user interface 56 the number of licenses purchased or held by a licensee can be changed by the administrator 55.

The different operations and functional blocks shown in Figure 4 are preferably implemented as software blocks, which are run by processor 46 by calling threads 44 in the application program 26 and protocol stack 28.

The present invention discloses a method by which license control can be handled in a simple manner by performing it below the protocol stack (in view of the server hierarchy). In a WAP gateway server any requirement of using many separate license systems for all combinations of the WAP protocol are avoided by the present invention. A license control system could also be implemented above or within the WAP stack, but would lead to separate license control systems for different protocol combinations. The remote client, i.e. the terminal can make a connection to the WAP server using any of the layers or using many combinations of the protocols. For example, looking at Figure 1, protocol combinations WDP+WTLS (for services that only require datagram transport with security) , WDP+WTP (for applications that only require transaction services without security), WDP+WTP+WSP (for applications that do not require security, but otherwise normal WAP sessions), WDP+WTLS+WTP (for applications that only

require transaction services with security) and WDP+WTLS+WTP+WSP (full WAP stack) are all possible and they would all need own licensing counting system, if implemented above the stack. If license control would be implemented above or within the WAP stack, also the problem that not all protocols do use sessions at all, would arise and would need to be solved. For example implementing a licensing system that limits the maximum number of concurrent WSP sessions is easy, but there is also connectionlesss WSP protocol that does not use sessions at all. The present invention, by checking the remote address and remote port information below the protocol stack in every data packet solves this problem in a general way.

The invention can be implemented as software, which when loaded into a computer will function as a gateway server according to the present invention. The functionality of the license control according to the invention can be programmed e.g. in the C or Java programming language, or any other programming language.

This paper presents the implementation and embodiments of the invention with the help of examples. It is obvious to a person skilled in the art, that the invention is not restricted to details of the embodiments presented above, and that the invention can be implemented in another embodiment without deviating from the characteristics of the invention. For example, although the foregoing is a related to mobile terminals browsing the Internet or a WAP proxy, it is to be understood that the communication may be of different types including sending and receiving information, conducting transactions such as financial transactions sending and receiving electronic mail or messages. The range of activities includes accessing services, for example weather reports, news, stock prices, flight schedules, downloading ringing tones, banking services including information provision and payments. It may occur in communications environments other than the Internet and may also be used with other protocol stacks than WAP. Thus, the presented embodiments should be considered illustrative, but not restricting. Hence, the possibilities of implementing and using the invention are only restricted by the enclosed patent claims. Consequently, the various options of implementing the

invention as determined by the claims, including the equivalent implementations, also belong to the scope of the present invention.

Claims

1. A method of controlling, at a server, access right of a message received from a terminal at the server, and where the message is processed by a protocol stack (50), the method comprising:

checking the right of the message to enter the server before the message is allowed to pass to the protocol stack (50).

2. A method according to claim 1, wherein the message is a data packet comprising

a sender address specifying the address of the terminal,

a port number specifying the application address of the instance sending the message at the terminal, and

user data including the contents of the message,

and the method further comprises

reading both the sender address and the port number from the data packet for identifying the terminal.

3. A method according to claim 1, wherein the method further comprises:

communicating messages with a particular wireless network and for adapting messages received from the wireless network for the protocol stack (50), and after the adaptation performing the checking of the access right.

4. A method according to claim 2, wherein the method further comprises:

establishing a session between the server and the terminal and for receiving the data packet within the session,

reserving a license for the session as a response to having determined existance of access right, and

monitoring the time passed since the last data packet arrived in one session, and releasing the license for the session where a predetermined time has passed since the last data packet arrived in the session.

5. A method according to claim 2, wherein the method further comprises:

storing a number (Y) of access right licenses purchased by a licensee, and

reserving a license (C) for each different combination of sender address and port number found in a data packet, and

controlling that the number of reserved licenses (C) does not exceed the number of purchased access right licenses (Y).

6. A method according to claim 1, wherein the method further comprises:

passing the message to the protocol stack (50) in response to determining allowed access, and

discarding the message in response to determining denied access.

7. A method according to claim 6, wherein the method further comprises:

returning an error message to the terminal in response to a discarded message.

8. A method according to claim 4, wherein where the license has been released for a particular session and a data packet again arrives in that session, performing the access right checking for the newly received data packet and reserving a new license upon allowed access.

9. A method according to claim 4, wherein where a data packet arrives before said predetermined time has passed, performing the access right checking for the newly received data packet, and allowing access on basis of the already reserved license without reserving a new license.

10. A method according to any preceding claim in which the terminals comprise mobile terminals, for example cellular telephones, supporting the Wireless Application Protocol (WAP).

11. A server for receiving a message from a terminal and comprising a protocol stack (50) for processing the message according to a particular protocol stack, the server further comprising:

license control means (53) for controlling the access right of the message to enter the server before the message is allowed to pass to the protocol stack (50).

12. A server according to claim 11, wherein the message is a data packet comprising

a sender address specifying the address of the terminal,

a port number specifying the application address of the instance sending the message at the terminal, and

user data including the contents of the message,

and the server further comprises

means (53) for reading both the sender address and the port number from the data packet for identifying the terminal.

13. A server according to claim 11, wherein the server further comprises

a bearer adapter (51) for communicating messages with a particular wireless network and for adapting messages received from the wireless network for the protocol stack (50), and wherein the license control means (53) have been placed functionally below the protocol stack (50) and above the bearer adapter (51) in the server hierarchy.

14. A server according to claim 12, wherein the server further comprises

connection means (50 - 52) for establishing a session between the server and the terminal and for receiving the data packet within the session,

reservation means (53) for reserving a license for the session as a response to the license control means (53) having determined existance of access right, and

timing means (53) for monitoring the time passed since the last data packet arrived in one session, and releasing the license for the session where a predetermined time has passed since the last data packet arrived in the session.

15. A server according to claim 12, wherein the server further comprises

storage means for storing a number (Y) of access right licenses purchased by a licensee, and

means for reserving a license (C) for each different combination of sender address and port number found in a data packet, and

means for controlling that the number of reserved licenses (C) does not exceed the number of purchased access right licenses (Y).

16. A server according to claim 11, wherein server further comprises means (53) for passing the message to the protocol stack (50) in response to determining allowed access and for discarding the message in response to determining denied access.

17. A server according to claim 16, wherein server further comprises means (53) for returning an error message to the terminal in response to a discarded message.

18. A server according to any of claims 11-17 comprising a gateway server serving a plurality of mobile terminals.

19. A server according to claim 18 comprising a WAP gateway.

20. A computer program product for controlling, at a server, access right of a message received from a terminal at the server, and where the message is processed by a protocol stack (50), the computer program product comprising:

computer readable program means (53, 56, 63) for controlling the access right of the message to enter the server before the message is allowed to pass to the protocol stack (50).

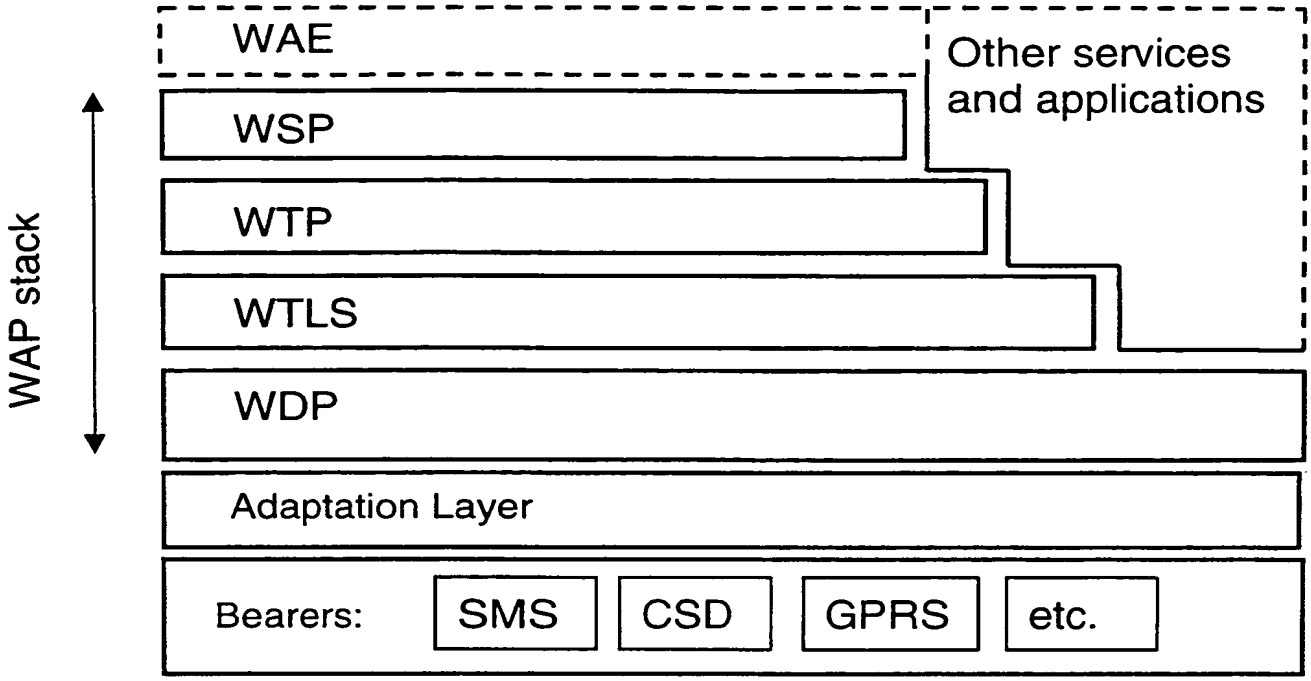

WAE
Other services and applications
WSP
WTP
WTLS
WDP
Adaptation Layer
Bearers:
SMS
CSD
GPRS
etc.
WAP stack

Fig. 1

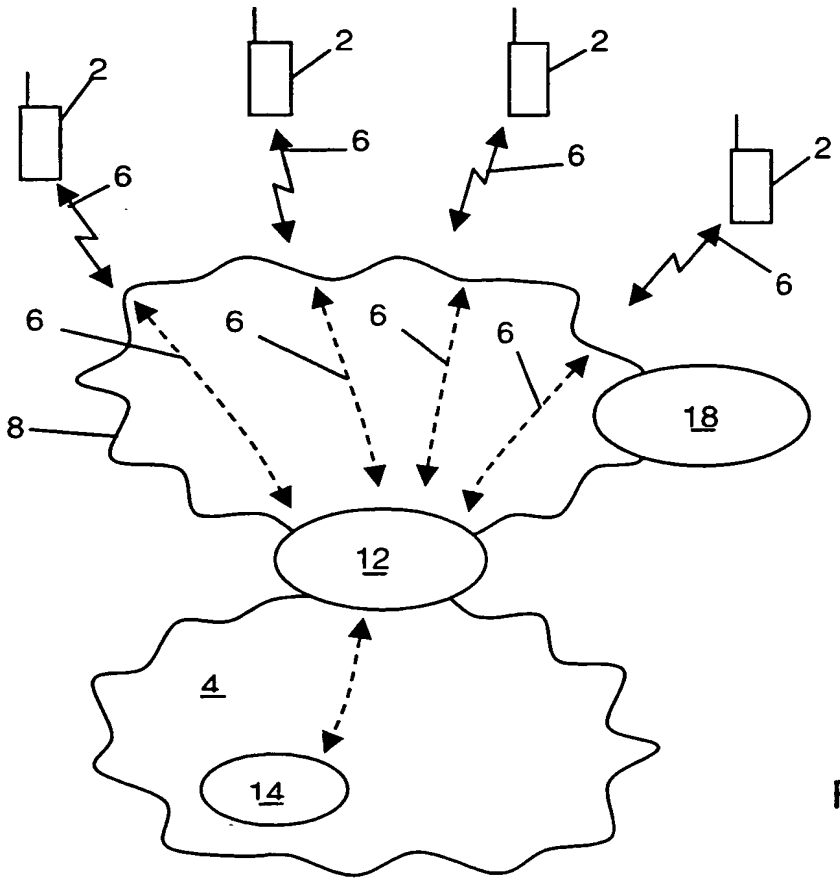

2
6
8
12
14
18
4

Fig. 2

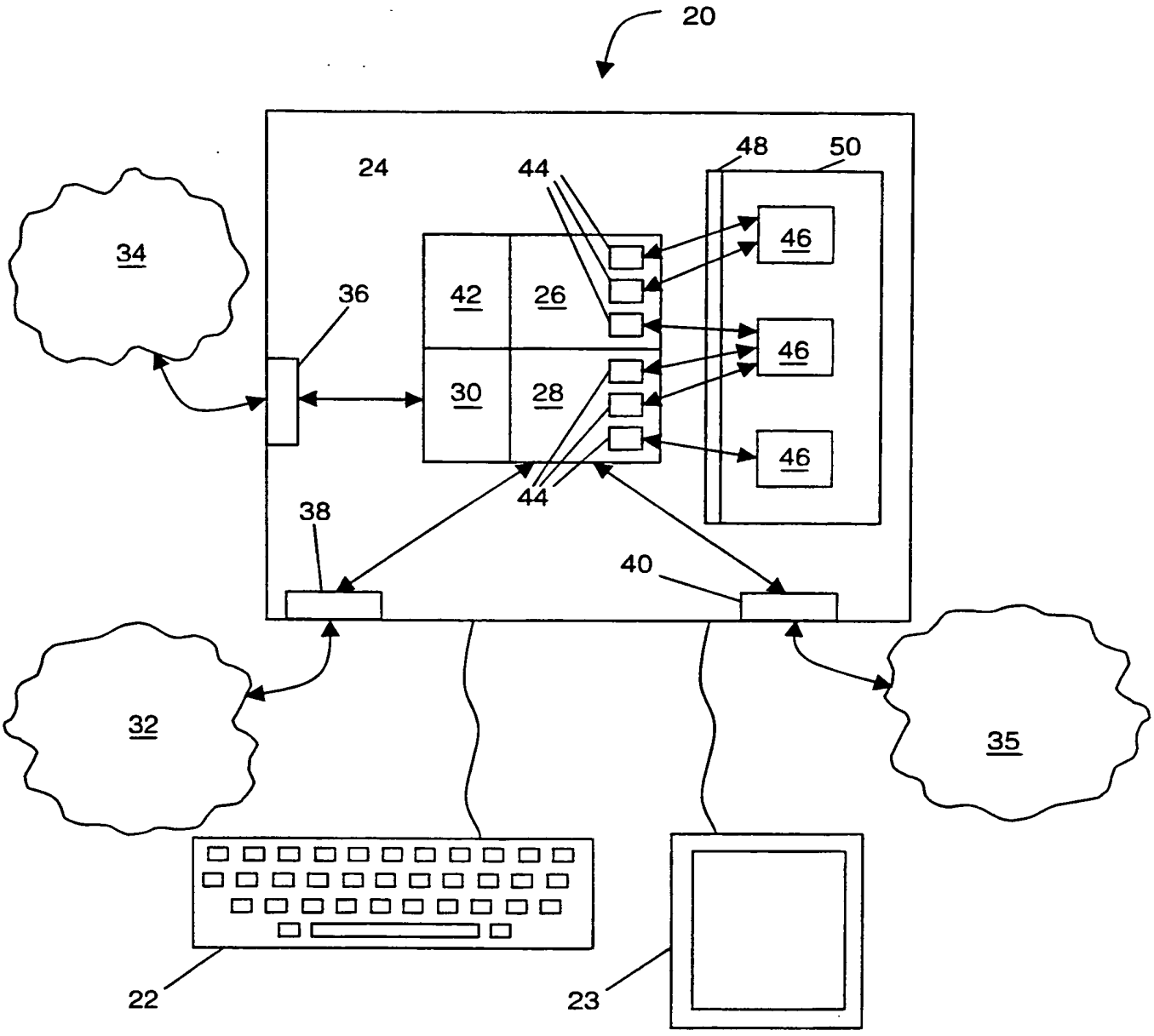


Fig. 3

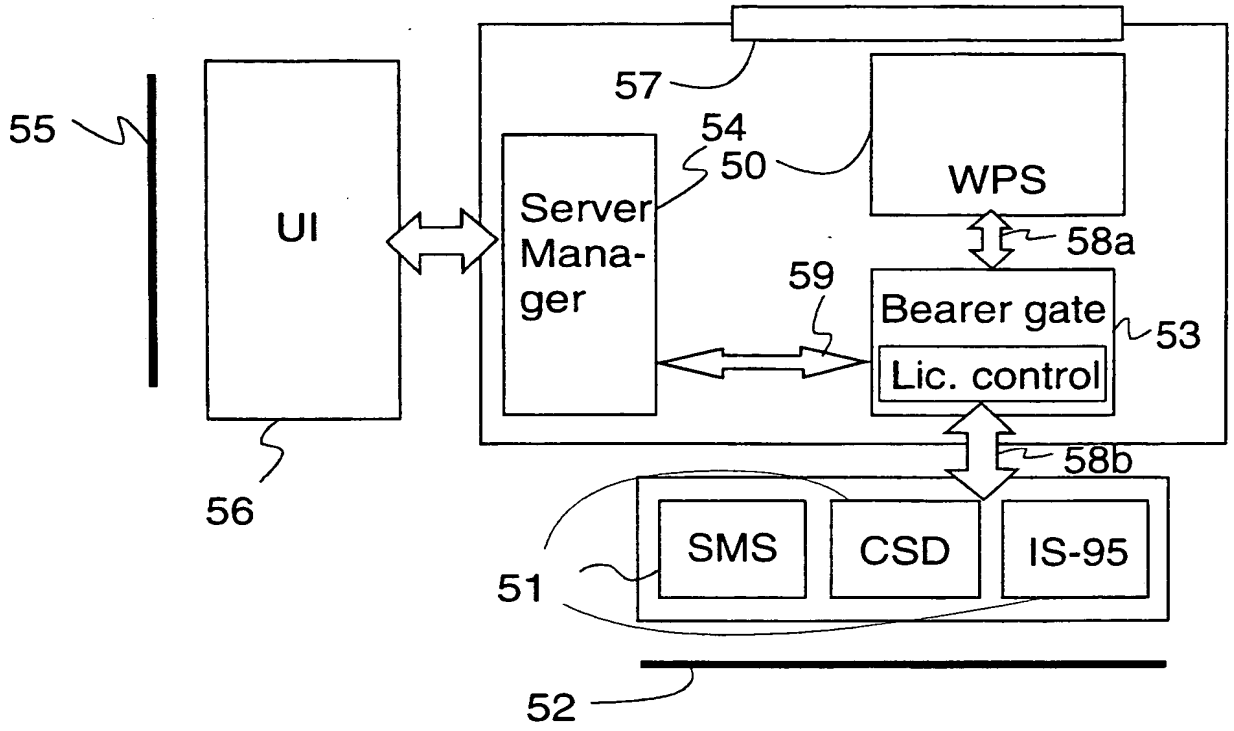

55
UI
56
57
54
50
Server Mana-ger
WPS
58a
59
Bearer gate
53
Lic. control
58b
SMS
CSD
IS-95
51
52

Fig. 4

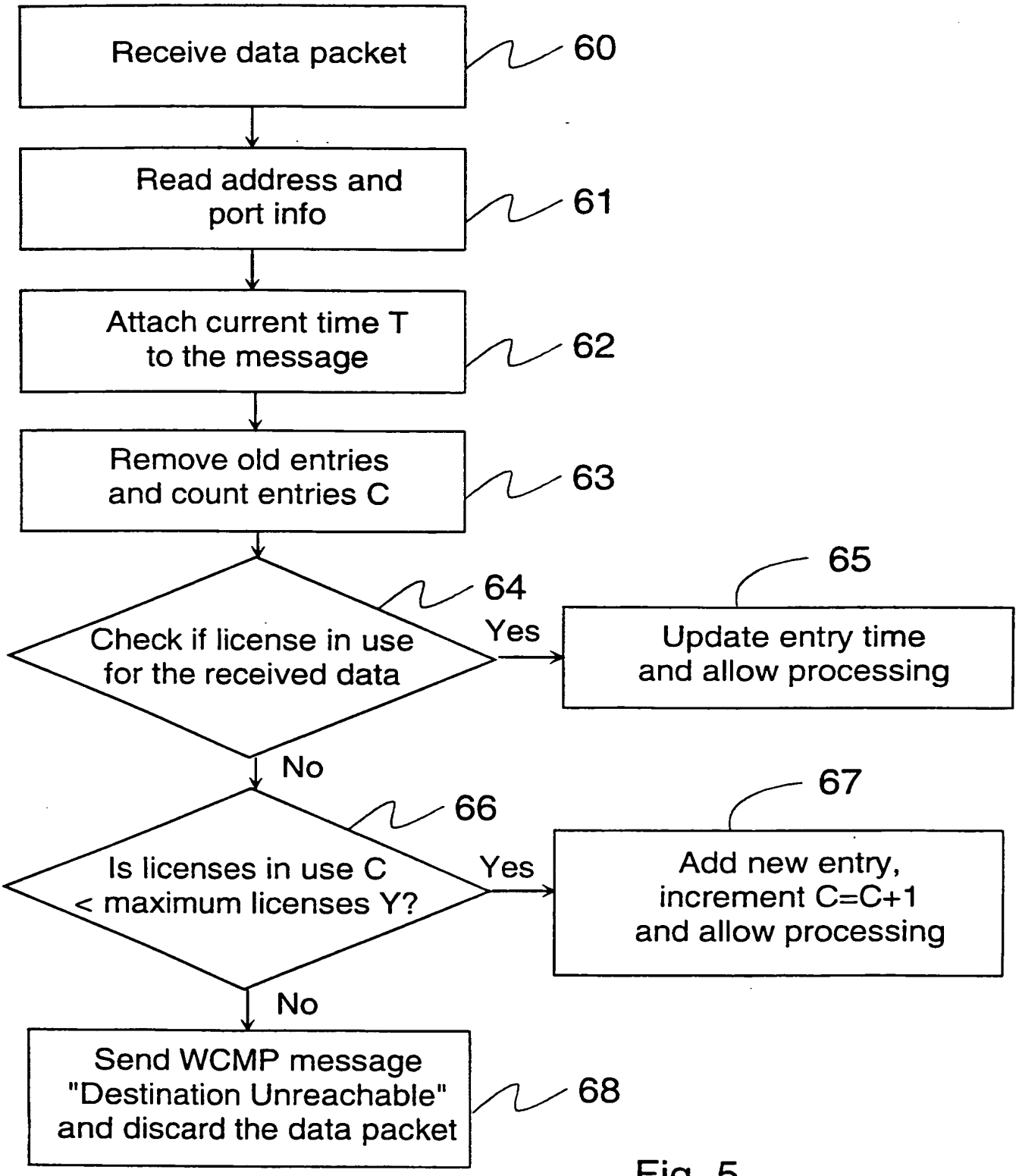

Receive data packet
60
Read address and port info
61
Attach current time T to the message
62
Remove old entries and count entries C
63
Check if license in use for the received data
64
Yes
Update entry time and allow processing
65
No
Is licenses in use C < maximum licenses Y?
66
Yes
Add new entry, increment C=C+1 and allow processing
67
No
Send WCMP message "Destination Unreachable" and discard the data packet
68

Fig. 5

INTERNATIONAL SEARCH REPORT

Interna. al Application No
PCT/FI 00/00513

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	WO 99 56431 A (NOKIA MOBILE PHONES LTD (F) 4 November 1999 (1999-11-04) page 5, line 13 -page 9, line 7; figure 3 abstract; claims 1-4	1-4, 6-14, 16-20
Y	---	5,15
Y	PATENT ABSTRACTS OF JAPAN vol. 1998, no. 10, 31 August 1998 (1998-08-31) & JP 10 136336 A (CANON INC), 22 May 1998 (1998-05-22) abstract	5,15

A	EP 0 642 283 A (NOKIA MOBILE PHONES LTD) 8 March 1995 (1995-03-08) page 1, line 1 -page 2, line 24 abstract	1-20

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 October 2000	29. 11. 2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Thomas Tholin

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internal Application No
PCT/FI 00/00513

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9956431 A	04-11-1999	AU 4360999 A	16-11-1999
JP 10136336 A	22-05-1998	US 6088737 A	11-07-2000
EP 0642283 A	08-03-1995	FI 933894 A	07-03-1995
		JP 7170579 A	04-07-1995
		US 5802465 A	01-09-1998

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.